

**ARTICOLI**

**Le definizioni di sistemi  
di intelligenza artificiale  
nelle proposte  
legislative europee.  
Un'analisi critica.**

---

**Giuseppe Proietti**

Dottorando di ricerca in diritto commerciale  
Università di Roma "Tor Vergata"

# Dialoghi di Diritto dell'Economia

---

## **Rivista diretta da**

Raffaele Lener, Roberto Natoli, Andrea Sacco Ginevri,  
Filippo Sartori, Antonella Sciarrone Alibrandi

## **Direttore editoriale**

Andrea Marangoni

## **Direttori di area**

### **Attività, governance e regolazione bancaria**

Prof. Alberto Urbani, Prof. Diego Rossano, Prof. Francesco Ciraolo, Prof.ssa Carmela Robustella,  
Dott. Luca Lentini, Dott. Federico Riganti

### **Mercato dei capitali finanza strutturata**

Prof. Matteo De Poli, Prof. Filippo Annunziata, Prof. Ugo Malvagna, Dott.ssa Anna Toniolo,  
Dott. Francesco Petrosino

### **Assicurazioni e previdenza**

Prof. Paoloefisio Corrias, Prof. Michele Siri, Prof. Pierpaolo Marano, Prof. Giovanni Maria Berti De Marini,  
Dott. Massimo Mazzola

### **Contratti di impresa, concorrenza e mercati regolati**

Prof.ssa Maddalena Rabitti, Prof.ssa Michela Passalacqua, Prof.ssa Maddalena Semeraro,  
Prof.ssa Mariateresa Maggiolino

### **Diritto della crisi di impresa e dell'insolvenza**

Prof. Aldo Angelo Dolmetta, Prof. Gianluca Mucciarone, Prof. Francesco Accettella, Dott. Antonio Didone,  
Prof. Alessio di Amato

### **Fiscalità finanziaria**

Prof. Andrea Giovanardi, Prof. Nicola Sartori, Prof. Francesco Albertini

### **Istituzioni dell'economia e politiche pubbliche**

Prof.ssa Michela Passalacqua, Prof. Francesco Moliterni, Prof. Giovanni Luchena, Dott.ssa Stefania Cavaliere,  
Dott. Lorenzo Rodio Nico

## Criteri di Revisione

I contributi proposti alla Rivista per la pubblicazione sono sottoposti a una previa valutazione interna da parte della Direzione o di uno dei Direttori d'Area; il quale provvede ad assegnare il contributo a un revisore esterno alla Rivista, selezionato, rationes materiae, fra professori, ricercatori o assegnisti di ricerca.

La rivista adotta il procedimento di revisione tra pari a singolo cieco (single blind peer review) per assicurarsi che il materiale inviato rimanga strettamente confidenziale durante il procedimento di revisione.

Qualora il valutatore esprima un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche, aggiunte o correzioni, la Direzione si riserva di negare la pubblicazione dell'articolo. Nel caso in cui la Direzione decida per la pubblicazione, deve verificare previamente che l'Autore abbia apportato le modifiche richieste dal Revisore.

Qualora il revisore abbia espresso un giudizio negativo, il contributo può essere rifiutato oppure inviato, su parere favorevole della maggioranza dei Direttori dell'area competente rationes materiae, a un nuovo revisore esterno per un ulteriore giudizio. In caso di nuovo giudizio negativo, il contributo viene senz'altro rifiutato.

**[\*] 1. Una breve premessa.**

La composizione di una nozione di "intelligenza artificiale" (IA) per finalità normative costituisce una operazione ardua.

Nonostante siano stati fatti diversi tentativi, più o meno validi, emerge sempre un qualche elemento che non consente di completare una definizione in senso empirico che rintracci un consenso unanime. Gli stessi tecnologi hanno tentato e tentano ancora oggi di fornire un quadro definitorio, ma il risultato finale trova sempre una qualche obiezione.

La ragione fondamentale risiede nel fatto che l'intelligenza artificiale non riflette una tecnologia specifica, bensì una scienza, una disciplina<sup>01</sup>. Più in particolare, una scienza dell'informatica che, quindi, al suo interno contiene diversi strumenti tecnologici, ciascuno dei quali possiede delle proprie caratteristiche tecniche, capacità e approcci<sup>02</sup>. Perciò, è difficile inserire tutti questi strumenti (che verranno chiamati "sistemi di intelligenza artificiale") all'interno di un'unica definizione. Per questa ragione, alcu-

---

\* Paper presentato nel corso del convegno del 20 ottobre 2023 organizzato da Consob e l'Università di Roma Tor Vergata "AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?" tenutosi presso le Scuderie di Palazzo Altieri in Roma.

01 Lo sviluppo delle tecnologie nel nuovo millennio ha affinato la scienza biomedica e la scienza informatica formando così una nuova scienza che studia l'intelligenza artificiale. Questo sviluppo ha dato anche vita alla formulazione di un nuovo linguaggio. Si veda in tal senso G. ALPA, AA.VV. *diritto e intelligenza artificiale*, Alpa (a cura di), Pisa, 2020, p. 13. In letteratura alcuni sottolineano che lo scopo di questa disciplina non risiederebbe nel replicare o simulare l'intelligenza umana, ma di riprodurla o emularla; in tal senso si veda M. SOMALVICO, F. AMIGONI, V. SCHIAFFONATI, *Intelligenza artificiale*, in *Storia della scienza*, S. Petruccioli (a cura di), vol. IX, Roma, Istituto della Enciclopedia Italiana, 2003, p. 615.

02 Ad esempio, sulla tematica dei cc.dd. *Software agents*, che si differenziano dai *software* tradizionali, già ne discutevano ampiamente F. BRAVO, *Contratto cibernetico*, in *dir. inf. e inform.*, n. 2/2011, pp. 169 e ss.; G. SARTOR, *Gli agenti software: nuovi soggetti*, in *Contratto e impresa*, n. 2/2022, pp. 466 e ss.

ni inquadrano la IA come un "termine ombrello"<sup>03</sup> o un "concetto riassuntivo"<sup>04</sup>. Va da sé che una definizione legislativa più è ampia e flessibile, più riesce a ricomprendere tutti i sistemi al suo interno, anche se una soluzione di questo genere deve fare i conti con il requisito della inclusività e della precisione.

L'attuale campo dell'IA è, quindi, una combinazione di più campi di ricerca, ognuno con il proprio obiettivo, i propri metodi e le proprie situazioni applicabili<sup>05</sup>. Si tratta di campi tra loro correlati, con il pericolo di trascurare le loro differenze fondamentali e di riferirsi indiscriminatamente a tutti loro come IA<sup>06</sup>.

Il legislatore europeo è stato uno dei primi a tentare di fornire una definizione normativa di sistemi di IA attraverso la proposta tramutata nel c.d. *Artificial Intelligence Act (AIA)*<sup>07</sup>. Tuttavia, come si vedrà di seguito, la Commissione europea, il Consiglio d'Europa e il Parlamento europeo hanno fornito ipotesi definitorie tra loro differenti e, ad oggi, questo tema è uno dei più dibattuti all'interno del trilatero che sta interessando le istituzioni<sup>08</sup>. Si è giunti a questa fase dopo un percorso europeo intrapreso a partire dal 2017.

## 2. L'AIA e il mercato digitale in fase di regolamentazione.

I dibattiti che negli ultimi anni si sono sviluppati sul tema dell'innovazione in seno alle istituzioni euro-

03 H. RUSCHEMEIER, *AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal*, ERA Forum, 2023, p. 364; vd. altresì F. CABITZA E L. FLORIDI, *Intelligenza Artificiale*, Milano, 2021, pp. 29-30. L'A., inoltre, propone di considerare la IA come una forma di "automazione", ossia, l'esecuzione automatica di compiti che, solitamente richiedono una certa intelligenza per essere eseguiti dagli esseri umani.

04 In quest'ultimo senso depone l'ultimo Quaderno giuridico Consob, *AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?*, F. CONSULICH, M. MAUGERI, C. MILIA, T.N. POLI, G. TROVATORE (a cura di), 2023, p. 7. Nel documento si legge, infatti, che il termine intelligenza artificiale rappresenta un concetto "riassuntivo", la cui «utilità risiede nell'aggregare sul piano lessicale programmi che utilizzano differenti metodi ma che appaiono tutti accomunati dal medesimo elemento funzionale: la capacità di elaborare quantità enormi di dati in tempi estremamente ravvicinati, minimizzando i tempi di latenza e contribuendo così alla soluzione efficiente di problemi che normalmente richiederebbero il concorso di diversi attori umani muniti di competenze eterogenee.»

05 PEI WANG, *On Defining Artificial Intelligence*, *Journal of Artificial General Intelligence* 10(2)1-37, 2019.

06 *Ibidem*.

07 Lo ha anticipato il legislatore brasiliano che con la legge n. 21/2020 all'art. 2 ha fornito la seguente definizione di sistema IA: «o sistema baseado em processo computacional que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões e recomendações ou tomar decisões que influenciam ambientes reais ou virtuais». Tradotto, sta a significare che un sistema di intelligenza artificiale sarebbe un «sistema basato su un processo computazionale che può, per un dato insieme di obiettivi definiti dall'uomo, fare previsioni e raccomandazioni o prendere decisioni che influenzano ambienti reali o virtuali».

08 L'ultimo incontro del trilatero è stato programmato per la data del prossimo 6 dicembre 2023.

pee hanno segnato un importante traguardo il 21 aprile del 2021 con la presentazione della proposta di Regolamento sull'intelligenza artificiale (o *Artificial Intelligence Act*) da parte della Commissione europea.

Prima di quella data l'Unione Europea aveva emanato una serie di atti non vincolanti volti alla definizione dell'approccio alle nuove tecnologie, in modo particolare all'intelligenza artificiale (di seguito anche IA).

La prima iniziativa da parte dell'UE in materia di intelligenza artificiale è rintracciabile nella risoluzione del Parlamento europeo del febbraio 2017 con la quale sono state fornite raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica<sup>09</sup>. In specie, il Parlamento si era prefigurato l'obiettivo di individuare un punto di equilibrio che potesse sostenere l'innovazione e la competitività industriale mantenendo al contempo un'elevata sicurezza e tutela dei diritti e delle libertà dei cittadini.

Successivamente, la Commissione europea è intervenuta con una relazione con cui delineava una ridefinizione dell'industria europea alla luce delle nuove sfide emergenti dalle tecnologie<sup>10</sup>.

La stessa istituzione, a seguito della costituzione dell'*European Group on Ethics in Science and New Technologies*, stilava la relazione "*Artificial Intelligence, Robotics and 'Autonomous' Systems*", con l'intento di descrivere le problematiche derivanti dai più recenti sviluppi tecnologici, risaltando in particolare le implicazioni etiche e morali<sup>11</sup>.

Nel mese di aprile del 2018 la Commissione ha adottato la comunicazione dal titolo "L'intelligenza artificiale per l'Europa". Il documento programmatico definiva gli obiettivi di investimento, nonché quelli legislativi ed etici nell'ambito del quadro dell'innovazione europea<sup>12</sup>. L'UE ha perciò focalizzato l'attenzione anche sui profili etici derivanti dall'utilizzo di sistemi di IA.

Sempre nell'ambito di atti non vincolanti, sono stati elaborati dei principi da parte del c.d. Gruppo di

<sup>09</sup> Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), consultabile su [eur-lex.europa.eu](http://eur-lex.europa.eu)

<sup>10</sup> *Re-finding industry, Report from the High-Level Strategy Group on Industrial Technologies*, consultabile al sito [op.europa.eu](http://op.europa.eu)

<sup>11</sup> *Artificial Intelligence, Robotics and 'Autonomous' Systems*, relazione consultabile al sito [op.europa.eu](http://op.europa.eu)

<sup>12</sup> *L'intelligenza artificiale per l'Europa*, 2018, Comunicazione consultabile al sito [ec.europa.eu](http://ec.europa.eu)

esperti ad alto livello<sup>13</sup> che hanno portato all'adozione della comunicazione della Commissione europea intitolata "Creare fiducia nell'intelligenza artificiale antropocentrica" con la quale sono stati recepiti<sup>14</sup>.

Il prelude all'emanazione della proposta dell'*Artificial Intelligence Act* è stato "Il libro bianco sull'intelligenza artificiale" pubblicato il 19 febbraio 2020<sup>15</sup>.

Ulteriori e recenti interventi sono stati adottati dal Parlamento europeo e dal Consiglio d'Europa. Il Parlamento europeo ha adottato due risoluzioni. La prima, datata 20 ottobre 2020, recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate; la seconda, in pari data, recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale<sup>16</sup>.

Il Consiglio d'Europa è intervenuto con un documento attraverso cui ha evidenziato la rilevanza di determinare i sistemi di IA da considerare ad alto rischio<sup>17</sup>. In un altro documento, del 21 ottobre 2021, dal titolo *The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, ha posto in risalto le problematiche e i rischi derivanti dall'opacità, dalla complessità dei sistemi di IA, nonché dai pregiudizi che comportano un ampio grado di imprevedibilità<sup>18</sup>.

Si è così giunti alla proposta di Regolamento del 2021 in cui la premura principale – a fronte dei vantaggi, ed al contempo dei rischi, derivanti dalla diffusione dell'IA – risiede nella creazione di un ecosistema di fiducia da parte degli utenti garantendo la sicurezza e i diritti umani, senza pregiudicare gli investimenti e la ricerca<sup>19</sup>.

<sup>13</sup> *Orientamenti etici per una IA affidabile*, 8 aprile 2019, consultabile al sito [digital-strategy.ec.europa.eu](https://digital-strategy.ec.europa.eu)

<sup>14</sup> *Creare fiducia nell'intelligenza artificiale antropocentrica*, consultabile al sito [eur-lex.europa.eu](https://eur-lex.europa.eu)

<sup>15</sup> *White paper*, consultabile al sito [ec.europa.eu](https://ec.europa.eu); sui temi affrontati nel documento sia consentito il rinvio a G. PROIETTI, *Il libro bianco sull'intelligenza artificiale. L'approccio europeo tra diritto ed etica*, in *Giustiziacivile.com*, 24 giugno 2020.

<sup>16</sup> Entrambe le risoluzioni sono consultabili al sito [europarl.europa.eu](https://europarl.europa.eu)

Per un quadro sull'intervento del Parlamento europeo si veda U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della commissione europea*, in *Riv. dir. Civ.*, n. 6/2020, pp. 1274-1276.

<sup>17</sup> consultabile al sito [consilium.europa.eu](https://consilium.europa.eu)

<sup>18</sup> *Council of the European Union, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020, consultabile al sito [consilium.europa.eu](https://consilium.europa.eu)

<sup>19</sup> L'ultima Opinione resa dalle istituzioni europee sulla proposta di AIA è stata resa dall'EDPS il 23 ottobre 2023 con "Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments" consultabile al sito [edps.europa.eu](https://edps.europa.eu)

Dunque, si inserisce esattamente in questa dimensione tattica l'ultima iniziativa della Commissione europea nell'ambito della strategia sull'innovazione, la quale risalta per la sua pregnanza giacché costituisce la prima iniziativa con cui si concretizza quell'approccio che fino ad aprile 2021 veniva stilato solamente a livello programmatico.

L'AIA (*Artificial Intelligence Act*) rappresenta la prima iniziativa legislativa al mondo con la quale si ambisce ad una regolamentazione generale di tale tecnologia e uno degli obiettivi è quello di ridurre il *gap* esistente con altri Stati in termini di sviluppo e investimenti.

Sotto un profilo squisitamente geopolitico, l'UE tenta di avere una voce in capitolo in materia di innovazione (stante la grande differenza in termini di sviluppo tecnologico con super potenze come USA e Cina) attraverso iniziative normative che possano creare il c.d. *effetto Bruxelles* generatosi in buona parte con il GDPR.

Sebbene il presente contributo non possa costituire la sede di analisi di altre iniziative legislative, occorre segnalare che l'intero quadro deve comunque affiancarsi ad altri recenti interventi del legislatore adottati nell'ambito del mercato digitale europeo. Alcuni di questi, sebbene riguardino la materia dei dati personali, hanno una diretta incidenza rispetto alle questioni attinenti alle innovazioni tecnologiche. Alcuni progetti legislativi sono stati già approvati – il riferimento è al *Digital Service Act*, al *Digital Market Act*, al *Data Governance Act* e al Regolamento di esecuzione *Open Data* – mentre altri sono ancora in una fase di discussione. Il riferimento è al *Data Act*. Ciò senza voler considerare le ulteriori normative in materia di cybersicurezza.

Le iniziative legislative, sebbene riguardino ciascuna aspetti e ambiti particolari, preannunciano un sistema ampiamente regolato con un processo di decodificazione sempre più incisivo. L'auspicio è che ciò non irrigidisca eccessivamente il sistema.

### **3. Cos'è l'intelligenza artificiale?**

Come si è accennato, la disciplina dell'intelligenza artificiale fa riferimento ad un ampio numero di strumenti computazionali applicati nei più svariati settori della società. Comprendere quali sono realmente



gli strumenti che rientrano nella nozione di IA è una operazione non semplice<sup>20</sup>.

Il termine "intelligenza artificiale" viene unanimemente ascritto al matematico John McCarthy che, nel 1956, la definì come «scienza e ingegneria della costruzione di macchine intelligenti»<sup>21</sup>.

Sebbene McCarthy abbia coniato il termine, molti individuano in A. Turing il padre di computer intelligenti e, quindi, di quella che sarebbe poi divenuta l'intelligenza artificiale. Fu nel 1947 che Turing per la prima volta parlò di *computer intelligence* nel corso di un seminario tenutosi a Londra<sup>22</sup>. Ma ancor prima, già nel 1943, gli scienziati McCulloch e Pitts proposero un loro modello di neurone artificiale che oggi costituisce la base delle reti neurali, benché la formalizzazione del modello di apprendimento venne effettuata sei anni più tardi da Hebb attraverso quel modello che ancora oggi porta il suo nome<sup>23</sup>.

Il percorso storico di questa scienza è stato travagliato. Dall'introduzione del nuovo termine di IA gli studiosi hanno sin da subito iniziato ad interrogarsi sulla possibilità di parlare di *intelligenza* in riferimento a macchine e su quanta analogia ci possa essere fra queste ultime e l'uomo<sup>24</sup>.

Nel corso degli anni '60 vennero pubblicati i primi contributi scientifici in cui sono stati individuati vari limiti che la ricerca sull'intelligenza artificiale effettivamente ha poi incontrato negli anni a venire; in particolar modo, per la forte differenza esistente fra i risultati cognitivi ottenuti dalle macchine e quelli tipici degli esseri umani.

Infatti, nel 1969, gli scienziati M. Minsky e S. Papert evidenziarono i limiti delle prime reti neurali artificiali da loro realizzate. La levatura intellettuale e culturale degli autori provocò, quindi, un declino dell'entusiasmo creatosi attorno a questo argomento determinando una consistente riduzione dell'in-

---

20 Si pensi alla tecnologia *blockchain*. Alcuni la ritengono una particolare tipologia di intelligenza artificiale, mentre altri escludono si tratti di IA. In senso affermativo, N. ABRIANI e G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale*, Bologna, 2021, p. 30; in senso negativo, G. PASCERI, *Intelligenza artificiale, algoritmo e machine learning*, Milano, 2021, p. 24.

21 H. RUSCHEMEIER, *op. cit.*, p. 363. L'A. rileva come molte delle definizioni che sono state successivamente elaborate intorno al termine di intelligenza artificiale siano state sempre incentrate su un agire umano, un pensare umanamente o razionalmente.

22 M. GABBRIELLI, *Dalla logica al deep learning: una breve riflessione sull'intelligenza artificiale*, in AA.VV. *XXVI lezioni di diritto dell'intelligenza artificiale*, U. Ruffolo (a cura di), Torino, 2021, p. 24. Si è discusso di *computer intelligence* nel moderno senso di macchina capace di imparare dall'esperienza.

23 *Ivi*, p. 25.

24 R. CINGOLANI - D. ANDRESCIANI, *Robots, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive*, in AA.VV. *Diritto e intelligenza artificiale*, Alpa (a cura di), Pisa, 2020, p. 29.

teresse scientifico ed economico nei confronti dell'IA fino ai primi anni '90<sup>25</sup>. Questo è stato il periodo che viene identificato come il c.d. inverno dell'intelligenza artificiale, quello tra gli anni '70 e '80<sup>26</sup>.

Perciò, fu solo negli anni '90 che la ricerca nel campo dell'IA riprese vigore grazie all'accelerazione delle tecnologie elettroniche e all'aumento delle prestazioni dei computer<sup>27</sup>.

Oggi si riscontra un interesse e un'attenzione notevole nei confronti della materia dovuta all'impatto sociale, politico ed economico che lo sviluppo di alcuni sistemi possono comportare. In particolare, sono sostanzialmente tre i fattori che hanno determinato il crescente interesse di cui si discute. Il primo, riguarda lo sviluppo tecnico di alcuni sistemi, confluito nell'apprendimento automatico (*machine learning*), il quale ha segnato il passaggio da una tecnologia algoritmica tradizionale ad una più complessa inerente per l'appunto all'apprendimento automatico (anche con modelli di calcolo sub-simbolico); il secondo, riguarda lo sviluppo di *hardware* con potenze di calcolo grandemente superiori rispetto al passato<sup>28</sup>; il terzo, è costituito da una enorme quantità di dati a disposizione prima inimmaginabile<sup>29</sup>. Questi ultimi sono fondamentali per il funzionamento dei sistemi IA costituendo il loro "carburante"<sup>30</sup>.

---

25 Ivi, p. 30. Gli autori sottolineano come in questi anni ci si è concentrati in particolar modo sull'agente intelligente come entità autonoma e si sono moltiplicati gli studi sui *software* intelligenti e sugli agenti intelligenti *embodied* in un sistema fisico. Negli scienziati si è quindi rinnovata la speranza di costruire robot intelligenti, di inserire cioè un'intelligenza artificiale in un corpo sintetico per imitare l'essere umano.

26 M. GABBRIELLI, *op. cit.*, p. 25. Si è trattato di un periodo in cui, dopo le aspettative forse eccessive degli anni '60 ha visto la delusione di molti per i mancati risultati e la conseguente drastica riduzione dei finanziamenti.

27 R. CINGOLANI – D. ANDRESCIANI, *op. cit.*, p. 30.

28 L'aumento della velocità di calcolo e della capacità di immagazzinamento dei dati ha consentito la realizzazione di dispositivi elettronici sempre più sofisticati che hanno determinato l'attuale rivoluzione digitale. Internet, motori di ricerca, telefonia mobile, social network, *Big Data*, Industria 4.0, sanità digitale, modelli previsionali in ambiti finanziari, sociali, sanitari, climatologici, che sono tutte conseguenze dirette o indirette dell'evoluzione tecnologica dei *transistor*. L'unità di misura di calcolo è rappresentata dai cc.dd. FLOP (*Floating point operation per second*), ovvero il numero di operazioni binarie al secondo che un computer è in grado di fare. I supercomputer più potenti oggi disponibili sono in grado di svolgere decine di *PetaFLOP*, vale a dire, decine di milioni di miliardi di operazioni al secondo. I computer con una maggior capacità di calcolo si trovano in Cina, Svizzera e USA. In tal senso, R. CINGOLANI – D. ANDRESCIANI, *op. cit.*, p. 27.

29 Si veda M. GABBRIELLI, *op. cit.*, p. 26; sulla rilevanza dei dati come unità fondamentale della nuova economia in cui è necessario bilanciare i diversi interessi dell'innovazione e dello sviluppo tecnologico con la stabilità finanziaria e la protezione dei consumatori, si veda R. LENER, *La consulenza finanziaria digitalizzata*, in AA.VV. *Liber amicorum* F. Vassalli, Torino, 2023, p. 315.

30 Sia consentito il rinvio a quanto già rilevato in G. PROIETTI, *Il trasferimento dei dati personali all'estero: proporzionalità, poteri delle agenzie di intelligence ed effetto bruxelles*, in *dir. inf. e inform.*, n. 2/2023 in corso di pubblicazione; si veda C. GRÖGER, *There is not AI without data*, in *Communications of the ACM*, 64(11), pp. 98-108, 2021

La particolarità dei sistemi IA risiede nel fatto che ad essi non vengono delegati compiti che tradizionalmente l'uomo ha delegato alle macchine (o agli animali) nel passato, ma fa riferimento ad attività che comportano una scelta tra un numero di opzioni, parole o categorie<sup>31</sup>. Si tratta di attività che, a loro volta, fanno parte di processi diretti al raggiungimento di obiettivi complessi in contesti reali caratterizzati da un alto contenuto di conoscenza, autonomia, giudizio e incertezza<sup>32</sup>.

Per valutare se sia legislativamente opportuno fornire una definizione di sistema di intelligenza artificiale e, in caso affermativo, quale potrebbe essere la soluzione più calzante (anche in virtù di quelle già fornite dai legislatori) è necessario avere chiari i connotati tecnici che differenziano un sistema da un altro<sup>33</sup>.

#### 4. (Segue) Le differenti tecniche e i diversi approcci nei sistemi IA.

Una prima distinzione che dovrebbe essere effettuata riguarda la IA *debole* (o limitata) e la IA *forte* (o generale). Anche per questa prima distinzione, però, non esiste ormai un'idea univoca e condivisa. Difatti, c'è chi ritiene i sistemi di IA *debole* vadano ascritti a quegli strumenti più risalenti i cui *output* dipendono esclusivamente da istruzioni prestabilite dai programmatori, mentre i sistemi di IA *forte* hanno la capacità di autoapprendimento e producono *output* autonomi<sup>34</sup>.

Invece, stando alla impostazione classica che operava questa distinzione, la IA *debole* farebbe riferimento ai sistemi utilizzati per risolvere compiti determinati, mentre la IA *forte* sarebbe identificata in quel sistema capace di emulare in tutto un essere umano e, quindi, in grado di agire nella generalità dei domini<sup>35</sup>.

In altri termini, i sistemi tecnologici attuali di IA vanno ascritti alla prima categoria, mentre la IA *forte*,

31 F. CABITZA E L. FLORIDI, *op. cit.*, p. 33

32 *Ibidem*.

33 H. RUSCHEMEIER, *op. cit.*, p. 364, come la gran parte degli autori in letteratura specifica come sia necessario e inevitabile differenziare i diversi tipi di IA a seconda delle differenti tecniche di cui si avvalgono.

34 Per una sintesi e elaborazione di questa impostazione si veda il Quaderno Consob AI e abusi di mercato cit., pp. 23-26.

35 Tale distinzione, tuttavia, diverge concettualmente da quella originariamente elaborata da John Searle, il quale inquadrava l'intelligenza artificiale forte in quei sistemi capaci di sviluppare una coscienza.

consistente nell'esecuzione della maggior parte delle attività che possono svolgere gli umani<sup>36</sup>, rimane ancora confinata alla teoria.

Alcuni hanno delineato la differenza tra le due forme di sistemi rilevando come la macchina *emula*, ma non *simula* alcune funzioni della mente umana; essa esegue compiti e prestazioni simili a quelli che comportano l'esercizio dell'intelligenza benché non siano dotati di una vera e propria intelligenza e, quindi, in grado di comprendere e riprodurre gli stati cognitivi della mente<sup>37</sup>.

L'intelligenza artificiale attuale, quindi *debole*, riesce a surclassare le capacità e le prestazioni umane in alcuni domini in cui opera, ma solo se circoscritta a tale specifico dominio, ovvero per l'esecuzione di singole operazioni (operazioni di calcolo, di gioco, di statistica, di strategia, di riconoscimento facciale ecc.). Attualmente non esiste ancora una forma di intelligenza artificiale generale<sup>38</sup> paragonabile a quella umana, ossia una capacità di riuscire ad operare in senso lato su molti o tutti i domini presentabili nella realtà<sup>39</sup>.

Pertanto, i riferimenti e le descrizioni tecniche dei sistemi di IA che verranno illustrati di seguito afferiscono esclusivamente a quella forma di IA *debole*.

---

<sup>36</sup> La ricerca è orientata al raggiungimento del comune ragionamento dei sensi, dell'autocoscienza e della capacità della macchina di definire il proprio scopo. Sul tema si veda il documento *dell'High-level expert group on artificial intelligence, A definition of Artificial Intelligence: main capabilities and scientific disciplines*, 8 aprile 2019, p. 5, consultabile sul sito [digital-strategy.ec.europa.eu](https://digital-strategy.ec.europa.eu); nella relazione si legge testualmente che «*a general AI system is intended to be a system that can perform most activities that humans can do. Narrow AI systems are instead systems that can perform one or few specific tasks. Currently deployed AI systems are examples of narrow AI. In the early days of AI, researchers used a different terminology (weak and strong AI). There are still many open ethical, scientific and technological challenges to build the capabilities that would be needed to achieve general AI, such as common sense reasoning, self-awareness, and the ability of the machine to define its own purpose*».

<sup>37</sup> A. CONTALDO E F. CAMPARA, *Intelligenza artificiale e diritto. Dai sistemi esperti "classici" ai sistemi esperti "evoluti": tecnologia e implementazione giuridica*, in *Intelligenza artificiale. Algoritmi giuridici lus condendum o "fantadiritto"?*, G. Taddei Elmi e A. Contaldo (a cura di), Pisa, 2020, p. 70; R. MARTINEZ, *Artificial intelligence: distinguishing between types & definitions*, 19 NEV. L.J., 2019, p. 1027, indica che mentre la IA *debole* simula, quella *forte* è semplicemente intelligenza, o come specifica l'autore, una effettiva istanziazione.

<sup>38</sup> Il filosofo N. Bostrom definisce l'intelligenza artificiale generale raffigurando «macchine all'altezza degli esseri umani quanto a intelligenza generale – cioè dotate di buon senso e di un'effettiva capacità di imparare, ragionare e pianificare per affrontare compiti complessi di elaborazione delle informazioni in una vasta gamma di domini naturali e astratti». Questo in N. BOSTROM, *Superintelligenza*, Bollati Boringhieri, 2018, p. 24.

<sup>39</sup> Le realtà tecnologiche con le quali oggi si tenta di superare tali limiti sono rappresentate dal c.d. *Swarm intelligence*, ovvero l'utilizzo di un corposo numero di agenti autonomi in cui ciascuno di essi contribuisce alla soluzione di uno specifico problema.

Per le differenti conseguenze giuridiche che ne possono derivare, una dicotomia che può essere operata è quella tra le strategie algoritmiche e quelle euristiche<sup>40</sup>. Ma, per semplificare, si possono dividere le tecniche dei sistemi IA più avanzati tra tecniche simboliche (chiamate GOFAI – *Good Old-Fashioned Artificial Intelligence*) che hanno dominato l'IA da metà anni 50' a fine anni 80' e quelle sub-simboliche;<sup>41</sup> ciò per evitare di confondere i sistemi IA con i *software* tradizionali che non rientrerebbero in questa categoria.

Partendo dalla visione *simbolica* e *dichiarativa* (IA "classica") tutti i sistemi potrebbero essere ricompresi in uno schema composto da tre fasi: (i) percezione; (ii) elaborazione; (iii) azione<sup>42</sup>.

La prima fase si caratterizza per l'acquisizione di dati e quindi della percezione della realtà esterna in cui opera (c.d. *knowledge based*). In altri termini, al sistema vengono forniti tutti quei dati e informazioni che saranno necessarie affinché possa operare<sup>43</sup>.

La seconda fase consta di quelle regole di inferenza (*inference engine*)<sup>44</sup>. Il sistema possiede un insieme

---

40 Le strategie euristiche si fondano sull'esperienza e impiegano tecniche che di fronte a un problema prospettano un ventaglio di risposte alternative. La soluzione dei problemi è ottenuta partendo da un numero finito di assiomi e seguendo regole d'inferenza determinate, cioè l'euristica che è un metodo con cui, ad imitazione del pensiero umano, viene sacrificata la certezza della soluzione ottimale ad un problema in favore di una ricerca più rapida che esplora solo i percorsi più promettenti e si accontenta di una buona soluzione. In questo senso, A. CONTALDO e F. CAMPARA, *op. cit.*, pp. 20-21. È stato infatti sottolineato come «per cercare di fronteggiare il (...) fenomeno dell'esplosione combinatoria», tipico degli ambienti complessi in cui agisce l'agente cibernetico, si fa normalmente ricorso a tecniche «euristiche», in grado di «migliorare l'efficienza della ricerca delle soluzioni (nello spazio di stati del problema), spesso sacrificandone (...) le caratteristiche di completezza e sistematicità (...) che rappresentano i principali vantaggi dell'uso di un sistema automatico (...). Infatti, per raggiungere il "goal" (obiettivo finale) proposto al sistema, non vengono esaminati tutti i percorsi possibili, "ma si esaminano prima (o solamente) quelli che sembrano più promettenti sulla base di criteri determinati, le c.d. funzioni euristiche", in questo senso, F. BRAVO, *op. cit.*, p. 179. Le strategie algoritmiche, invece, godono di un margine di esplorazione e di azione ridotta perché seguono uno schema predefinito per il raggiungimento di un predeterminato obiettivo. In tal senso si veda sempre F. BRAVO, *Contrattazione telematica e contrattazione cibernetica*, Milano, 2007, pp. 206 e ss.

41 Qui di seguito si seguirà la suddivisione operata dal matematico F. RIGUZZI, *Introduzione all'intelligenza artificiale*, ult. versione. 2021, <https://arxiv.org/abs/1511.04352>.

42 L'ISO negli Standard internazionali ISO/IEC 22989 del 2022 riguardanti *Information technology – Artificial intelligence – Artificial intelligence concepts and terminology*, consultabile al sito [iso.org](https://www.iso.org), definisce la IA simbolica come una intelligenza artificiale basata su tecniche e modelli che manipolano simboli e strutture secondo regole esplicitamente definite per ottenere inferenze.

43 Secondo M. Feigenbaum, la potenza di un programma intelligente nel risolvere un problema dipende primariamente dalla quantità e qualità di conoscenza che possiede su tale problema.

44 L'ISO negli Standard internazionali ISO/IEC 22989 cit. definisce l'inferenza come il ragionamento in base al quale le conclusioni sono derivate da premesse note.

di istruzioni necessarie che si traducono in meccanismi di ragionamento. Quest'ultimo può fondarsi su processi logico-deduttivi attraverso i quali dedurre conclusioni in forza delle conoscenze acquisite, oppure può basarsi su processi probabilistici e statistici. È grazie a questa fase di elaborazione dei dati e di conoscenza del problema che si può giungere alla terza fase dell'azione, che si può tradurre essenzialmente in un contenuto, previsione, decisione o raccomandazione.

In ogni caso, le tecniche simboliche avrebbero come obiettivo quello di automatizzare il ragionamento e l'azione rappresentando le situazioni che vengono analizzate per mezzo di simboli comprensibili per l'uomo ed elaborandoli attraverso algoritmi. Le tecniche sub-simboliche, invece, sono basate sulla riproduzione di fenomeni naturali e non rappresentano la conoscenza in modo direttamente comprensibile.

La ricerca, di recente, è orientata verso una combinazione di tecniche simboliche e sub-simboliche<sup>45</sup>. Tra le tecniche simboliche viene ricompresa la ricerca nello spazio degli stati<sup>46</sup> (una delle applicazioni di questa tecnica, ad esempio, è quella dei giochi), il ragionamento automatico<sup>47</sup> (nell'ambito del quale

---

45 F. RIGUZZI, *op. cit.*, p. 3.

46 *Ivi*, pp. 3-4: «questa tecnica viene utilizzata quando si vuole scegliere una serie di azioni che portino da uno stato iniziale a uno o più stati finali desiderati. Condizioni, affinché possa essere utilizzata, sono: che lo stato del mondo esterno possa essere rappresentato in maniera concisa (in forma simbolica), che le azioni disponibili possano essere espresse come regole per il passaggio da uno stato al successivo e che esista un test per stabilire se uno stato è finale». Le strategie utilizzate con questa tecnica possono essere "non informate" perché non utilizzano criteri per scegliere quale nodo espandere quando v'è ne è più di uno alla stessa profondità oppure "informate", le quali sono più efficienti poiché basate su una conoscenza specifica del problema. Tra queste ultime rientrano strategie euristiche, ossia che forniscono una stima e non un valore certo. Infine, la ricerca nello spazio può essere "in avanti" allorché parta da uno stato iniziale per perseguire uno stato finale, oppure "all'indietro" allorché partendo da uno stato finale arriva a quello iniziale; da ultimo, esiste anche un tipo di ricerca "bidirezionale" o "mista".

47 *Ivi*, p. 10: Per «ragionamento automatico s'intende l'utilizzo di conoscenza al fine di inferire nuova conoscenza. A questo scopo è necessario rappresentare la conoscenza in un formato memorizzabile da un calcolatore, e utilizzabile per effettuare inferenze. Questi requisiti restringono il formato di rappresentazione a linguaggi formali, ovvero linguaggi con una sintassi e una semantica definiti in maniera precisa. Uno dei linguaggi formali maggiormente studiati è quello della logica».

ci si può avvalere dei c.d. sistemi esperti<sup>48</sup>) e l'apprendimento automatico<sup>49</sup>. Lo sviluppo e il perfezionamento di quest'ultimo approccio ha segnato il diffuso interesse che negli ultimi anni ruota intorno alla IA. Tra gli impieghi principali dell'apprendimento automatico ci sarebbero l'estrazione di conoscenza e il miglioramento delle prestazioni di una macchina. La conoscenza estratta può poi essere utilizzata da una macchina come base di conoscenza di un sistema esperto, oppure dall'uomo, come il caso della scoperta di nuove teorie scientifiche.

Il miglioramento delle prestazioni di una macchina, invece, si avrebbe quando si incrementano le capacità percettive e motrici di un robot.

A loro volta le tecniche di apprendimento automatico si possono suddividere in simboliche e sub-simboliche<sup>50</sup>. Tra le prime viene ricompreso l'apprendimento induttivo, ossia «il sistema parte dai fatti e dalle osservazioni derivanti da un insegnante o dall'ambiente circostante, e li generalizza ottenendo conoscenza che, auspicabilmente, sia valida anche per casi non ancora osservati (induzione)»<sup>51</sup>. I si-

---

48 *Ivi*, p. 14: si tratta di sistemi «caratterizzati dall'essere dotati di una conoscenza che riguarda uno specifico campo, e dall'essere in grado di risolverne i problemi relativi, che un esperto sarebbe in grado di risolvere. (...) la conoscenza viene espressa sotto forma di programma logico, e il metodo di inferenza (...) è usato per trovare soluzioni al problema. (...) Lo sviluppo di un sistema esperto richiede la scrittura delle regole generali sul dominio, che devono essere raccolte intervistando un esperto del dominio stesso. Questo processo, conosciuto con il nome di estrazione di conoscenza, è risultato essere estremamente lungo e difficile. Al fine di automatizzarlo, è possibile usare l'apprendimento automatico». L'ISO negli Standard internazionali ISO/IEC 22989 cit., definisce il sistema esperto come un sistema di intelligenza artificiale che acquisisce, combina e sintetizza le conoscenze fornite da uno o più esperti umani in un dominio specifico per dedurre soluzioni ai problemi.

49 *Ivi*, p. 15: l'A. riporta quanto affermato da Simon nel 1984 che «ha dato la seguente definizione di apprendimento (...): "L'apprendimento consiste di cambiamenti del sistema che siano adattativi, nel senso che mettono in grado il sistema di svolgere lo stesso compito o compiti estratti dalla medesima popolazione in maniera più efficace ed efficiente la prossima volta". Di sicuro, al fine di realizzare macchine che possano dirsi intelligenti, è necessario dotarle della capacità di estendere la propria conoscenza e le proprie abilità in modo autonomo».

50 *Ivi*, p. 16.

51 *Ibidem*. L'A. aggiunge che nell'ipotesi dell'apprendimento induttivo «da esempi, l'insegnante fornisce un insieme di esempi e controesempi di un concetto, e l'obiettivo è quello di inferire una descrizione del concetto stesso. Un esempio è composto da una descrizione di una istanza del dominio del discorso e da una etichetta; quest'ultima può essere + se l'istanza appartiene al concetto da apprendere, o - se l'istanza non gli appartiene (controesempio). Un concetto, quindi, non è altro che un sottoinsieme dell'insieme di tutte le possibili istanze del dominio del discorso, o universo. L'insieme di esempi e controesempi forniti dall'insegnante prende il nome di training set. La descrizione del concetto che si vuole apprendere deve essere tale da potersi usare per decidere se una nuova istanza, non appartenente al training set, appartenga o meno al concetto. La descrizione del concetto deve essere quindi un algoritmo che, data in ingresso una descrizione dell'istanza, restituisca in uscita +, se l'istanza appartiene al concetto, o -, se l'istanza non appartiene al concetto. Nel primo caso si parla di esempio appartenente alla classe positiva e nel secondo di esempio appartenente alla classe negativa».

stemi di apprendimento induttivo possono essere differenziati in virtù del linguaggio con il quale si possono descrivere le istanze e i concetti, i quali sono sostanzialmente i "linguaggi attributo valore"<sup>52</sup> e i "linguaggi del primo ordine". Ai primi corrispondono, come linguaggi di descrizione dei concetti, gli alberi di decisione e le regole di produzione, mentre ai secondi corrispondono descrizioni dei concetti anch'esse del primo ordine<sup>53</sup>.

Tra le tecniche sub-simboliche<sup>54</sup> vengono ricompresi approcci e tecniche come le reti neurali<sup>55</sup>, gli algoritmi genetici<sup>56</sup> e l'intelligenza degli sciami<sup>57</sup>.

È nell'ambito delle reti neurali che è stato elaborato il c.d. *deep learning*. Infatti, grazie all'incremento della potenza di calcolo dei computer (negli ultimi 30 anni) sono state addestrate reti con un numero

---

52 I linguaggi attributo valore hanno alcune limitazioni: essi non sono adatti a descrivere istanze costituite di sottoparti e aventi relazioni tra le sottoparti.

53 Gottlob Frege (1848-1925) fu il primo a sviluppare un sistema di assiomi e regole per la logica del primo ordine, superando così i limiti imposti dai sillogismi e dalla logica proposizionale. L'A., p. 19, rileva come i sistemi di apprendimento «sia da linguaggi attributo valore che da programmi logici, hanno avuto una vasta gamma di applicazioni, che va dalla diagnosi di malattie alla predizione della relazione struttura-attività nella progettazione di medicine, alla predizione della carcinogenicità delle sostanze chimiche. Con l'aumento della quantità di dati che vengono memorizzati ogni giorno dalle aziende e dalle organizzazioni in generale, gli algoritmi di apprendimento sono sempre più importanti in quanto consentono di estrarre da questa massa di dati informazioni nascoste, nuove e potenzialmente utili. Si parla in questo caso di data mining, ovvero di estrazione di conoscenza da dati grezzi».

54 L'ISO negli Standard internazionali ISO/IEC 22989 cit. definisce la IA sub-simbolica come quella intelligenza artificiale che si basa su tecniche e modelli che utilizzano una codifica implicita delle informazioni, che possono derivare dall'esperienza o dai dati grezzi.

55 *Ivi*, p. 20: Il modello del neurone attualmente più diffuso è chiamato neurone sigmoideale ed è costituito da un'unità con  $n$  ingressi numerici e una uscita numerica. Questo modello si comporta in maniera simile a un neurone naturale: ovvero si "attiva" quando riceve gli ingressi "giusti" e si "disattiva" in corrispondenza di ingressi "sbagliati".

56 *Ivi*, p. 24: L'A. rileva che «gli algoritmi genetici possono essere utilizzati anche per svolgere compiti di apprendimento automatico. In questo caso occorre rappresentare le descrizioni del concetto da imparare come sequenza di simboli: la fitness sarà data dall'accuratezza con la quale una descrizione del concetto classifica gli esempi del training set. Gli algoritmi genetici hanno avuto numerose applicazioni in biologia, ingegneria e nelle scienze fisiche e sociali. Una delle più interessanti consiste nella programmazione automatica, ovvero nella generazione automatica di programmi per calcolatore per risolvere un certo problema. In questo caso il genotipo degli individui è costituito da alberi che rappresentano un singolo programma in un dato linguaggio di programmazione. L'operatore di incrocio consiste nel sostituire un sottoalbero di un genitore con un sottoalbero dell'altro genitore».

57 *Ivi*, pp. 24-25: «gli algoritmi basati sull'intelligenza degli sciami (*swarm intelligence*) cercano di riprodurre il comportamento degli insetti che vivono in colonie, come formiche, api, termiti e vespe. (...) Algoritmi basati sulla riproduzione di sciami sono stati efficacemente utilizzati in numerosi ambiti: ad esempio, per il problema del commesso viaggiatore, per l'indirizzamento dei pacchetti di dati nelle reti informatiche, per l'indirizzamento di veicoli nella rete stradale e per l'assegnazione di lavorazioni su macchinari».



sempre maggiore di strati neurali; da qui il termine di reti "profonde" (*deep*)<sup>58</sup>. Il successo del *deep learning* è dovuto alla sua applicazione in molti campi, tra cui la visione artificiale, il riconoscimento del parlato, la traduzione automatica, la bioinformatica, la progettazione di medicine e l'analisi di immagini mediche<sup>59</sup>.

Sotto un profilo giuridico, o meglio, di rilevanza giuridica, una delle differenze più importanti riguarda quei sistemi che non riescono ad essere trasparenti. Infatti, alcuni sistemi come il *machine learning*, il *deep learning* e le reti neurali non sarebbero in grado di fornire spiegazioni sul loro operato<sup>60</sup>. A tal proposito esiste la nota dicotomia tra sistemi *glass box* e *black box*<sup>61</sup>.

## 5. Le diverse politiche del diritto.

Gli approcci alla regolamentazione di una tecnologia come la IA possono essere i più differenti. A fronte di chi sostiene una legislazione generale e orizzontale, altri la criticano ritenendo opportuna una normativa settoriale. Chi sostiene l'inutilità di una regolamentazione con un approccio generale fonda la propria tesi sulla ragione che i sistemi di IA sollevano problemi differenti a seconda del soggetto che li utilizza, del contesto e dello scopo<sup>62</sup>. Questo renderebbe superfluo fornire un'unica definizione omnicomprensiva della IA. Ciò che sarebbe necessario – sempre secondo questa impostazione – risiederebbe in un discernimento a seconda delle diverse caratteristiche dei vari algoritmi e applicazioni dei

---

58 Ivi, p. 22.

59 Ibidem.

60 A. CONTALDO e F. CAMPARA, *op. cit.*, p. 24.

61 Oggi gran parte degli algoritmi «di nuova generazione non si limita a dedurre in maniera deterministica conseguenze da assiomi prefissati dal programmatore, ma in virtù di sistemi automatici di apprendimento (c.d. machine learning), essi stessi producono gli stessi criteri di inferenza. Criteri che in molti casi non sono comprensibili agli stessi programmatori». In questo senso, A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, p. 78. Sul tema della *black box* si veda altresì F. PASQUALE, *The Black Box Society. The secret Algorithms That Control Money and Information*, Cambridge-London, 2015; CERQUITELLI, QUERCIA e PASQUALE, *Transparent Data Mining for Big and Small Data*, New York, 2017; GUIDOTTI, MONREALE, RUGGIERI, PEDRESCHI, TURINI, GIANNOTTI (2018). *Local Rule-Based Explanations of Black Box Decision Systems*, in arXiv:1805.10820; GUIDOTTI, MONREALE, RUGGIERI, PEDRESCHI, TURINI, GIANNOTTI (2019). *Meaningful Explanations of Black Box AI Decision System, Proceedings of the AAAI Conference on Artificial Intelligence*, 33(01), 9780-9784. <https://doi.org/10.1609/aaai.v33i01.33019780>

62 Tra questi H. RUSCHEMEIER, *op. cit.*, pp. 365 -366 che pone l'esempio "macroscopico" della differenza tra un sistema d'arma autonomo e un filtro *antispam*. Si pone l'interrogativo sull'opportunità per il legislatore di adottare un approccio di disciplina della IA nel suo complesso o per applicazioni in settori specifici anche G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. Trim. dir. pubb.*, n. 4/2022, p. 1087.

sistemi IA nel loro utilizzo pratico<sup>63</sup>.

Non manca chi, invece, ritiene che il discernimento che si deve operare riguardi quei sistemi i cui comportamenti sono già predefiniti nella fase di progettazione rispetto a quelli in cui la conoscenza viene derivata dalla loro esperienza allorché iniziano a funzionare<sup>64</sup>.

L'intero discorso si interseca inevitabilmente anche con il principio di neutralità tecnologica<sup>65</sup>. Infatti, viene da più parti segnalato come questo principio, consolidato nel dibattito internazionale, fa sì che una norma non debba far riferimento a una determinata tecnologia affermata in un particolare periodo storico<sup>66</sup>. Il vantaggio derivante dall'esplicazione del principio risiederebbe nel fatto che in questo modo il diritto non influenzerebbe il mercato favorendo l'una o l'altra tecnologia, non condizionerebbe lo sviluppo della tecnica e non la rincorrerebbe. Non ci si concentra sulla "cosa" ma sul "come", sposando quindi un approccio funzionale<sup>67</sup>. Nel nostro ordinamento è persino già presente una disposizione che definisce il principio in tesi, ovvero, l'art. 4, co. 2, lett. i), d.lgs. n. 259 del 2003 relativo al Codice delle comunicazioni<sup>68</sup> elettroniche il quale fa riferimento a un principio di «neutralità tecnologica, inteso come non discriminazione tra particolari tecnologie, non imposizione dell'uso di una particolare tecnologia rispetto alle altre e possibilità di adottare provvedimenti ragionevoli al fine di promuovere taluni servizi indipendentemente dalla tecnologia utilizzata»<sup>69</sup>. La logica di questo principio si inserisce a pieno

63 *Ibidem*. L'A. rileva peraltro come le definizioni di IA che si è tentato di fornire sinora non rispetterebbero i criteri di inclusività, precisione, completezza, praticabilità e permanenza delle definizioni giuridiche.

64 P. WANG, *op. cit.*, pp. 1-15. L'A. sembra far riferimento a un discernimento tra i sistemi che seguono un approccio algoritmico tradizionale rispetto all'apprendimento automatico. Questi dovrebbero essere governati da regole differenti.

65 Nel quaderno Consob IA e abusi di mercato cit., p. 97, si legge che la capacità dei sistemi di AI più avanzati «sembrerebbe incrinare l'applicazione del principio di neutralità tecnologica in sede di regolamentazione («*same risk, same activity, same treatment*») e il raggiungimento di un *level playing field*, cui tende peraltro l'intera disciplina in materia di intermediazione finanziaria».

66 G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. It., Collana Intelligenza artificiale e diritto*, E. Gabrielli e U. Ruffolo (a cura di), luglio 2019, pp. 1670 e ss. L'A., sotto un altro angolo prospettico, riguardante il rapporto tra tecnica e diritto, rileva come il diritto è chiamato a stabilire gli obiettivi e la tecnica deve invece essere il mezzo per raggiungerli. In tal senso, G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *dir. inf. e inform.*, n. 4-5/2012, p. 838.

67 *Ibidem*.

68 Così come sostituito dall'art. 1, co. 1, D.lgs. 8 novembre 2021, n. 207, come corretto dal Comunicato del 9 febbraio 2022, pubblicato nella G.U. 9 febbraio 2022, n. 33, che ha sostituito gli articoli da 1 a 98 con gli articoli da 1 a 98-tricies.

69 Sulla neutralità tecnologica si veda anche R. LENER, *op. cit.*, p. 315.

titolo in quella della tesi contraria ad una definizione di sistema di IA. In questo senso sembra deporre la linea programmatica in discussione in seno alle istituzioni del Regno Unito che intende, stando agli ultimi documenti ufficiali pubblicati, regolare - in modo settoriale e non orizzontale - l'utilizzo che se ne fa di una determinata tecnologia e non la tecnologia in sé<sup>70</sup>.

Continuando l'esplorazione delle varie tesi dottrinali, alcuni ritengono che sussista una differenza ragguardevole tra quelle che sono le definizioni fornite dai ricercatori rispetto a quelle fornite dalle istituzioni politiche<sup>71</sup>. Ciò che viene suggerito, quindi, consiste nell'elaborazione di una definizione che sia in grado di mantenere una maggiore fedeltà alle definizioni fornite dagli esperti del settore e che sia orientata a una (i) inclusione delle tecnologie attualmente in uso e delle applicazioni future; (ii) accessibilità per un pubblico non esperto; (iii) possibilità di implementare procedure di segnalazione e supervisione<sup>72</sup>.

Proprio sulla base di questi ultimi presupposti, parte della dottrina anglosassone pone all'attenzione quelli che sono i parametri principali per elaborare una definizione giuridica ottimale in ottemperanza ai principi di certezza del diritto e di proporzionalità<sup>73</sup>.

I parametri sono costituiti dalla (i) inclusività; (ii) precisione; (iii) comprensibilità; (iv) praticabilità e (v)

---

70 Anche nel Regno Unito si discute da tempo di una legislazione che in qualche modo riguarda i sistemi di IA anche se non è stata ancora avanzata una proposta legislativa ufficiale. Nei documenti di fonte governativa che sono stati adottati si riscontra proprio un approccio differente rispetto a quello europeo, focalizzato sull'uso dei sistemi e non sulla regolamentazione della tecnologia in sé, con un'impronta a favore dell'innovazione. Perciò il principale e recente documento è intitolato *A pro-innovation approach to AI regulation* consultabile al sito gov.uk; per un raffronto tra modello dell'UE e modello inglese si veda P. HACKER, *op. cit.*, p. 3. L'A. evidenzia come il Regno Unito sia orientato verso un modello di autoregolamentazione, enfatizzando la sicurezza dell'IA e i rischi. Ciò avverrebbe basandosi in gran parte sulla regolamentazione settoriale esistente, con un ambito normativo meno prescrittivo e dando alle aziende tecnologiche un maggiore margine di manovra per innovare, pur puntando al rispetto dei principi generali di sicurezza. Questo si estrinsecerebbe attraverso linee guida e standard volontari che le aziende sono incoraggiate a seguire, senza alcun obbligo. L'attenzione del Regno Unito, aggiunge l'autore, include una visione a lungo termine che considera non solo l'impatto immediato dell'IA, ma anche i suoi potenziali sviluppi futuri, compreso l'avvento teorico dell'Intelligenza Generale Artificiale (AGI). In senso favorevole, quindi, la politica britannica è volta a coltivare un ecosistema normativo flessibile; in senso critico, invece, verrebbero trascurati i rischi attuali dell'IA, come la discriminazione, l'opacità, e l'imprevedibilità.

71 P. M. KRAFFT, M. YOUNG, M. KATELL, K. HUANG, G. BUGINGO, *Defining AI in Policy versus Practice*, (2019) *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society (AIES)*, pp. 6-7.

72 *Ibidem*.

73 Il riferimento è a J. SCHUETT, *Defining the scope of AI regulations*, in *Law, Innovation and Technology*, Vol. 15, Issue 1, 2021, p. 1.

flessibilità. Stando a questa tesi, quando non viene rispettato il requisito della inclusività creando uno squilibrio in eccesso, si finisce per includere strumenti che non necessiterebbero di una regolazione; sarebbe invece per difetto quando la definizione legale è troppo ristretta e finirebbe per non ricomprendere fattispecie che dovrebbero essere incluse nella regolazione<sup>74</sup>.

Sotto il profilo della inclusività in eccesso potrebbe ricomprendersi un aspetto da più parti condiviso riguardante il pericolo che si corre approcciandosi ad una definizione legislativa di IA derivante proprio dall'utilizzo del termine "intelligenza", il quale finirebbe per antropomorfizzare il concetto<sup>75</sup>. Quindi, se l'applicazione IA è tale quando conduce a risultati ai quali potrebbe condurre l'intelligenza umana, l'oggetto della regolazione risulterebbe estremamente ampio, ricomprendendo qualunque processo che si possa dire *intelligente*<sup>76</sup>. La precisione del dettato normativo sta a significare che dovrebbe essere possibile determinare con chiarezza se un caso particolare può essere sussunto all'interno di una specifica fattispecie normativa. La praticabilità e comprensibilità si riferiscono al fatto che dovrebbe essere individuabile con un minimo sforzo la suddetta sussunzione in forza di un linguaggio comune e semplice.

Infine, la flessibilità fa sì che la definizione normativa si possa facilmente adattare ai progressi tecnici<sup>77</sup>. Dunque, secondo l'A., nel contesto di una definizione del perimetro dell'ambito materiale della normativa, non sarebbe opportuno fare riferimento al termine IA, o meglio, secondo questa teoria, la locuzione può essere utilizzata sotto un profilo "comunicativo" ma non deve rivestire un ruolo sostanziale e significativo<sup>78</sup>. Secondo questa tesi l'approccio più opportuno sarebbe quello fondato sul rischio con cui si intende raggiungere gli obiettivi prefissati focalizzandosi su quelle attività che presentano i rischi più elevati e lasciando inalterate le attività a basso rischio<sup>79</sup>. Le fonti di rischio dovrebbero essere suddivise sulla base di una combinazione di tre categorie che tengano conto di approcci tecnici (come è fatto il sistema), applicazioni (per cosa viene utilizzato) e capacità (cosa può fare)<sup>80</sup>. Sebbene con una struttura

---

<sup>74</sup> Ivi, p. 7.

<sup>75</sup> G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale cit.*, p. 1087.

<sup>76</sup> *Ibidem*. Da un punto di vista definitorio di certi sistemi "intelligenti" occorre menzionare anche la tesi di Teubner, il quale riprende a sua volta una teoria di Latour, parlando di "attanti", ossia macchine, ma capaci di azione. Si veda a tal proposito A. BECKERS – G. TEUBNER, *Three liability regimes for artificial intelligence*, Hart, Oxford, 2021, pp. 25 e ss.

<sup>77</sup> J. SCHUETT, *Defining the scope of AI regulations, cit.*, p. 7.

<sup>78</sup> Ivi, p. 16.

<sup>79</sup> *Ibidem*.

<sup>80</sup> *Ibidem*.

differente, il legislatore europeo sta optando per una simile politica del diritto.

## **6. L'approccio fondato sul rischio.**

L'approccio legislativo scelto dalle istituzioni europee è quello fondato sul rischio, ossia di suddividere l'impianto regolatorio a seconda del livello di rischio di un determinato sistema e a seconda del soggetto coinvolto (utilizzatore – sviluppatore – fornitore – distributore).

Dopo aver delineato – all'art. 2 AIA – alcuni ambiti a cui il Regolamento non trova applicazione<sup>81</sup>, il legislatore illustra i vari livelli di rischio. Come si vedrà, si tratta di una identificazione del rischio individuata sulla base del settore, contesto e casi d'uso nei quali un determinato sistema IA è chiamato a operare. L'identificazione dei sistemi, sotto un profilo tecnico, la si può rinvenire solo nella parte dedicata alla nozione di sistema IA (art. 3 AIA).

Dunque, a fronte di un primo livello di rischio *inaccettabile* (l'art. 5 AIA disciplina le pratiche vietate), il fulcro della disciplina è dedicato ai sistemi IA ad alto rischio. Infine, vi è una ulteriore categoria rappresentata da quei sistemi a rischio limitato, per i quali si applicano solo alcune disposizioni del Regolamento riguardanti la trasparenza e un ultimo livello a basso rischio per il quale non sono previsti obblighi e prescrizioni particolari.

Secondo alcuni, in realtà, l'obiettivo del legislatore sarebbe quello di prevedere le diverse categorie di rischio per adottare un approccio basato sul contesto in cui il sistema opera<sup>82</sup>.

Le idee che si rintracciano in letteratura sono le più varie; c'è chi lo ritiene l'approccio regolatorio più corretto in cui la regola può essere strutturata in termini di liceità, di divieto, ovvero di possibilità di utilizzazione a certe condizioni in virtù della probabilità del verificarsi del danno, oppure del rischio che un

---

81 La proposta della Commissione europea esclude dall'applicazione del Regolamento quei sistemi sviluppati per scopi esclusivamente militari. Lo stesso art. 2 AIA prevede poi che per alcuni sistemi IA ad alto rischio rientranti in una delle normative elencate nella stessa disposizione, l'unico articolo del Regolamento applicabile sarebbe l'art. 84 AIA riguardante il riesame periodico dell'allegato III del Regolamento da parte della Commissione. Il Consiglio d'Europa ha aggiunto tra le esclusioni di cui all'art. 2. In particolare, al di là del settore militare, sono stati aggiunti la difesa e la sicurezza nazionale, oltre a quei sistemi che producono *output* esclusivamente per finalità di ricerca e di sviluppo e per scopi non professionali.

82 H. RUSCHEMEIER, *op. cit.*, p. 368.

determinato comportamento realizzi una compromissione di un dato valore da tutelare<sup>83</sup>. L'A. segnala come il Regolamento europeo piuttosto che il ricorso a un sistema a tutele successive, abbia preferito prevedere regole di protezione preventiva, funzionali a ridurre o azzerare la probabilità di violazioni<sup>84</sup>. Altri lo ritengono un approccio ragionevole ma suscettibile di miglioramento<sup>85</sup>.

Altri ancora si esprimono critici per il modello adottato<sup>86</sup>. Alcuni hanno evidenziato, in senso critico, la differenza esistente tra la proposta di AIA e il GDPR. Quest'ultimo fondato sul principio dell'*accountability* e il primo in cui è invece il legislatore a stabilire come occorre procedere volta per volta<sup>87</sup>. Inoltre, secondo tale impostazione, il sistema non sarebbe sufficientemente dinamico poiché la normativa regolerebbe le applicazioni IA, anche future, con la prospettiva di oggi<sup>88</sup>.

Dunque, per analizzare l'essenza del quadro regolatorio proposto dal legislatore sarà necessario introdursi nel dettato normativo in questione per quanto riguarda le definizioni di sistema IA in generale e di sistema IA ad alto rischio.

---

83 M. SCIACCA, *Algocrazia e sistema democratico. Alla ricerca di una mite soluzione antropocentrica*, in *Contratto e impresa*, n. 4/2022, pp. 1203 - 1204.

84 *Ibidem*.

85 J. SCHUETT, *op. cit.*, pp. 20 ss. L'A. sostiene che si debba esplicitare che il campo di applicazione della normativa non sia basato sul termine IA; si dovrebbe prendere in considerazione la possibilità di distinguere tra diversi approcci tecnici e quello di considerare una distinzione sulla base delle capacità di un sistema. P. HACKER, *op. cit.*, p. 6 sostiene che l'iniziativa legislativa nel suo complesso va nella giusta direzione soprattutto per quanto riguarda la trasparenza dell'uso dell'IA, la documentazione, la gestione continua del rischio e la qualità dei dati. Tuttavia, c'è ancora la necessità di migliorare alcuni profili, tra cui anche la definizione di sistema IA; la classificazione concreta come sistema ad alto rischio; la biometria; la regolamentazione dei modelli di fondazione e dell'IA generativa; la catena del valore dell'IA; la valutazione dell'impatto sui diritti fondamentali; i meccanismi di notifica e di azione; i codici di condotta e gli standard tecnici.

86 M. VEALE., F. ZUIDERVEEN BORGESIU, *Demystifying the Draft EU Artificial Intelligence Act*, in *Computers and Society*, 2021, p. 97.

87 G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale cit.* p. 1096.

88 *Ibidem*. L'A. rileva altresì che un sistema del genere fondato sul rischio potrebbe gravare eccessivamente con oneri amministrativi a carico di piccole imprese e *start-up*. Lo stesso campanello di allarme viene sollevato da P. HACKER, *AI Regulation in Europe: From the AI Act to Future Regulatory Challenges*, forthcoming in *Ifeoma Ajunwa & Jeremias Adams-Prassl (eds), Oxford Handbook of Algorithmic Governance and the Law*, Oxford University Press, 2024, il quale sottolinea che l'UE deve essere attenta a non "soffocare" le poche aziende di IA competitive a livello internazionale di cui dispone.

## **7. La proposta di Regolamento europeo sull'intelligenza artificiale.**

Come si è visto, con l'*Artificial Intelligence Act* è stato accolto un approccio fondato sul rischio. La disciplina applicabile, quindi, varia a seconda della categoria di rischio in cui viene iscritto un determinato sistema IA.

Prima di definire quando un sistema IA è da considerarsi ad alto rischio il legislatore (art. 3 della proposta) si è premurato di fornire una definizione di sistema di IA.

La Commissione europea, il Consiglio d'Europa e il Parlamento europeo hanno fornito proposte definitorie in parte differenti, ognuna delle quali presenta le rispettive (e fisiologiche) criticità che si analizzeranno qui di seguito.

Prima di ciò, tuttavia, occorre porre all'evidenza il fatto che nella relazione che accompagna la proposta legislativa della Commissione europea viene riferito che il «titolo I definisce l'oggetto del regolamento e l'ambito di applicazione delle nuove regole concernenti l'immissione sul mercato, la messa in servizio e l'utilizzo di sistemi di IA. (...)» Viene precisato, a proposito di quanto già sopra accennato, che la «definizione di sistema di IA nel quadro giuridico mira ad essere il più possibile neutrale dal punto di vista tecnologico e adeguata alle esigenze future, tenendo conto dei rapidi sviluppi tecnologici e di mercato relativi all'IA (...)». Pertanto, l'intento del legislatore sarebbe quello di salvaguardare in qualche modo il principio di neutralità tecnologica, sebbene poi vada a definire in maniera piuttosto puntuale la tipologia di tecnologia che intende normare.

## **8. (Segue) La proposta della Commissione europea.**

La Commissione europea con il testo proposto il 21 aprile 2021, propone la seguente definizione di Sistema di IA all'art. 3: «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

Nell'allegato I a cui la Commissione fa rinvio vengono inserite le seguenti tecniche e i seguenti approcci: «a) approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning);

b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della

conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti;

c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione».

Si tratta con ogni evidenza di una struttura normativa complessa perché tiene in considerazione vari elementi per la composizione di una nozione che necessita di semplicità e flessibilità. Gli elementi fondanti la nozione della Commissione possono essere così riassunti: (i) *Software*; (ii) tecniche e approcci dell'allegato I; (iii) Obiettivi definiti dall'uomo; (iv) *output*; (v) contenuti, previsioni, raccomandazioni o decisioni; (vi) influenza degli ambienti di interazione. Ciascuno di questi elementi meriterebbe una dissertazione a sé.

In sintesi, l'indicazione del solo (i) *software* - che di per sé viene citato più volte dal legislatore nell'ambito di varie discipline senza che trovi una definizione univoca ad esso dedicata, salvo recenti proposte - lascerebbe immotivatamente fuori dall'ambito di applicazione l'elemento dell'*hardware*<sup>89</sup>. Quindi, stando così le cose, il legislatore considererebbe "il cervello" (i cc.dd. *Softbot*) della macchina ma non considererebbe i sistemi robotici, ossia quei casi in cui oltre al "cervello" ci sia "il corpo" (*Robot*).

Per quanto attiene alle (ii) tecniche e agli approcci di cui all'allegato I, nell'operare un rinvio ad un allegato, l'intento del legislatore sembrerebbe essere quello di garantire una certa flessibilità alla definizione rispetto al rapido mutamento del progresso tecnologico. In altri termini, le modifiche degli allegati normativi verrebbero affidati ad atti esecutivi della Commissione che, per il loro processo semplificato di adozione consentirebbero di stare al passo con la tecnica. Da un lato, verrebbe sacrificato l'*iter* democratico di una modifica normativa, ma dall'altro verrebbe salvaguardata la flessibilità della norma che verrebbe presto adattata agli sviluppi tecnici.

---

89 Una definizione di *software* viene formulata con la proposta relativa ad un'altra iniziativa legislativa europea, ossia la proposta di Regolamento relativo ai requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il Regolamento (UE) 2019/1020, meglio noto come *European Cyber Resilience Act*. La definizione proposta di *software* è la seguente (art. 3): «parte di un sistema di informazione elettronico costituita da un codice informatico». Nello stesso testo viene proposta la seguente definizione di *hardware*: «un sistema di informazione elettronico fisico, o parti di esso, in grado di trattare, conservare o trasmettere dati digitali». In dottrina si è affermato che, nell'ambito dell'informatica, per *software* si intende «l'insieme composito del "sistema operativo" e di tutti i programmi in esso presenti, mentre il programma per elaboratore consiste in una sequenza di istruzioni, espresse in linguaggio informatico che, per effetto del caricamento in un elaboratore, interagendo con il sistema operativo di quest'ultimo comporta lo svolgimento di determinate attività». In tal senso, E. M. INCUTTI, *La tutela giuridica del software: il caso Top System*, in *Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale*, S. Orlando e G. Capaldo (a cura di), Sapienza Università Editrice, 2022, p. 139.



Per altro verso, le varie tecniche e gli approcci che vengono indicati cercano di coprire tutte quelle realmente applicate nella realtà, benché alcune di esse vengano rappresentate con superfetazioni normative e potrebbero trovare una illustrazione più semplice e lineare.

A titolo esemplificativo, alla lett. a) sarebbe stato sufficiente l'indicazione dell'apprendimento automatico, così come alla lett. b) probabilmente ci si sarebbe potuti limitare all'indicazione degli approcci basati sulla logica, conoscenza e rappresentazione che a loro volta includono o possono includere i motori inferenziali, il ragionamento simbolico e i sistemi esperti. Le tecniche e gli approcci di cui alla lett. c), invece, come è stato correttamente rilevato, rischierebbero di includere *software* che hanno poco in comune con i sistemi IA più avanzati e i rischi da loro derivanti<sup>90</sup>. L'inserimento dell'Allegato I è stato sin da subito criticato da alcune istituzioni europee come il Comitato economico e sociale europeo<sup>91</sup>.

L'indicazione di (iii) "obiettivi definiti dall'uomo" potrebbe essere considerata ridondante e non inclusiva. Sotto quest'ultimo aspetto, non sarebbe inclusiva perché rimarrebbero fuori tutti quei casi in cui invece l'obiettivo verrebbe definito (anche in un processo decisionario successivo rispetto a quello originario) dalla macchina; ridondante in quanto il riferimento potrebbe essere del tutto evitato, visto che la fonte da cui provengono le definizioni di determinati obiettivi che la macchina (o *software* stando al lessico della Commissione) è tenuta a perseguire e realizzare suscitano poco interesse, ovvero se dall'uomo o dalla macchina stessa o da altra macchina.

Il riferimento (iv) agli *output* potrebbe essere inteso come "risultati" e, anche in questo caso, non si ravvedono solide ragioni per le quali dovrebbero specificarsi quali siano tali risultati come fa il legislatore prevedendo che essi devono essere (v) contenuti, previsioni, raccomandazioni o decisioni. Da ultimo, l'influenza degli ambienti con cui interagiscono potrebbe porre problemi ermeneutici su cosa si debba intendere con "influenza", ossia, deve ritenersi sufficiente una semplice modifica anche della sola "interfaccia virtuale" oppure sarebbe necessario che sia influenzato l'agire dell'utilizzatore in forza di quel

<sup>90</sup> P. HACKER, *op. cit.*, p. 7.

<sup>91</sup> Secondo il Comitato economico e sociale europeo, la definizione di sistema IA, così come proposto dalla Commissione, ha dato origine a un dibattito tra gli studiosi secondo i quali alcuni esempi riportati nell'Allegato I non possono essere ricompresi nell'ambito della IA e rilevano, invece, l'assenza di alcune tecniche di IA. Il Comitato sottolinea peraltro che non ci sarebbe alcun valore aggiunto nell'Allegato I raccomandando quindi la sua eliminazione. Ha quindi proposto la seguente definizione: «per sistema di intelligenza artificiale (AI) si intende un software in grado di generare in modo automatico, per un determinato insieme di obiettivi definiti dall'uomo, risultati quali contenuti, previsioni, raccomandazioni o decisioni, influenzando l'ambiente con cui interagisce». Il riferimento è alla *opinion* resa dal Comitato in data 2 settembre 2021, consultabile al sito [eesc.europa.eu](https://eesc.europa.eu)

risultato (*output*)? Una piattaforma on-line che, attraverso un determinato algoritmo (rientrante nelle tecniche di cui all'allegato I), personalizza determinati contenuti per l'utente ha già di per sé influenzato l'ambiente (virtuale) con cui interagisce (soddisfacendo il requisito legislativo) oppure è necessario che l'utente venga influenzato da quel contenuto?<sup>92</sup> Una interpretazione letterale della norma e dei *considerando* farebbe propendere per la prima opzione, ma l'effetto richiesto come conseguenza dalla norma è suscettibile di generare questioni ermeneutiche poco utili<sup>93</sup>.

### 9. (Segue) La proposta del Consiglio d'Europa.

Il compromesso finale del Consiglio d'Europa è stato votato e approvato, sotto la presidenza ceca il 6.12.22 dopo quattro proposte di testo<sup>94</sup>.

Nella relazione che accompagna il testo emendato si legge che l'ambito di cui all'art. 3 relativo alla definizione di IA è stato ristretto ai sistemi sviluppati mediante approcci di apprendimento automatico e approcci basati sulla logica e sulla conoscenza.

Il Consiglio ha inoltre introdotto il titolo I *bis* che tiene conto dei casi in cui i sistemi possono essere utilizzati per molti scopi diversi (IA per finalità generali). L'art. 4 *ter* par. 1 prevede che determinati requisiti per i sistemi ad alto rischio si applicano anche a quelli per finalità generali. Un atto di esecuzione dovrebbe specificare come dovrebbero essere applicati in relazione a tali sistemi.

---

<sup>92</sup> L'esempio calato nel mondo on-line si presta a rendere più chiaro il concetto e per cogliere l'occasione di specificare che molte delle fattispecie riguardanti le piattaforme on-line ad oggi fuoriescono dall'ambito di applicazione dell'AIA per soggiacere invece al *Digital Services Act* (DSA) interessando in particolare i «sistemi di raccomandazione».

<sup>93</sup> Al considerando n. 6 della proposta si legge che «la nozione di sistema di IA dovrebbe essere definita in maniera chiara al fine di garantire la certezza del diritto, prevedendo nel contempo la flessibilità necessaria per agevolare i futuri sviluppi tecnologici. La definizione dovrebbe essere basata sulle principali caratteristiche funzionali del *software*, in particolare sulla capacità, per una determinata serie di obiettivi definiti dall'uomo, di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano l'ambiente con cui il sistema interagisce, tanto in una dimensione fisica quanto in una dimensione digitale. I sistemi di IA possono essere progettati per funzionare con livelli di autonomia variabili e per essere utilizzati come elementi indipendenti (*stand-alone*) o come componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (*integrato*) o assista la funzionalità del prodotto senza esservi incorporato (*non integrato*). La definizione di sistema di IA dovrebbe essere completata da un elenco di tecniche e approcci specifici utilizzati per il suo sviluppo, che dovrebbe essere tenuto aggiornato alla luce degli sviluppi di mercato e tecnologici mediante l'adozione da parte della Commissione di atti delegati volti a modificare tale elenco».

<sup>94</sup> Le precedenti sono state Portogallo e Slovenia.

All'art. 2, invece, è stato specificato che il Regolamento non si applica per quei sistemi con finalità militari, di difesa e di sicurezza nazionale. La normativa non si applica neppure a quei sistemi i cui *output* sono utilizzati esclusivamente ai fini di ricerca e sviluppo e per quelle persone che utilizzano l'IA per scopi non professionali, ad eccezione degli obblighi di trasparenza.

Il Consiglio d'Europa con il testo di Regolamento emendato propone la seguente definizione di Sistema di IA all'art. 3 dell'AIA: «un sistema progettato per funzionare con elementi di autonomia che, sulla base di dati e input forniti da macchine e/o dall'uomo, deduce come raggiungere una determinata serie di obiettivi avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e produce output generati dal sistema quali contenuti (sistemi di IA generativi), previsioni, raccomandazioni o decisioni, che influenzano gli ambienti con cui il sistema di IA interagisce».

Dunque, il testo proposto dal Consiglio d'Europa abroga l'Allegato I e introduce un elemento di novità rappresentato da una nuova definizione, ossia quella riguardante i sistemi di IA per finalità generali: «un sistema di IA che, indipendentemente dalla modalità con cui è immesso sul mercato o messo in servizio, anche come software open source, è destinato secondo le intenzioni del fornitore a svolgere funzioni di applicazione generale quali il riconoscimento di immagini o vocale, la creazione di audio o video, la rilevazione di modelli, la risposta a domande, la traduzione o altro; un sistema di IA per finalità generali può essere utilizzato in una varietà di contesti e può essere integrato in una varietà di altri sistemi di IA».

Con la formulazione proposta dal Consiglio la struttura rimane complessa e le potenziali problematiche non sembrano dissolversi. Infatti:

(i) Tra gli elementi di novità si fa immediatamente notare il riferimento al *sistema* che prende il posto del *software*; quindi, un riferimento più ampio che può essere equiparato ad uno *strumento* che, perciò, considera anche la componente *hardware*.

(ii) Uno degli elementi innovativi più rilevanti però è rappresentato dall'introduzione dell'elemento

dell'*autonomia* che dischiude importanti interrogativi su cosa si intenda con questo elemento<sup>95</sup>. La tecnica, infatti, conosce vari gradi autonomia, con una costante supervisione dell'uomo fino ad arrivare a quel sistema totalmente autonomo<sup>96</sup>. Una interpretazione sistematica del Regolamento, in particolare con l'art. 14 AIA<sup>97</sup>, dovrebbe indurre a pensare ad una autonomia pur sempre accompagnata dalla supervisione umana.

(iii) Viene introdotto il riferimento ai *dati e input* che sono elementi scontati nell'ambito dei cc.dd. sistemi intelligenti (o agenti intelligenti) e, come si è visto sopra, rappresentando la *knowledge based*. Senza questi dati non esisterebbe alcun sistema di IA<sup>98</sup>.

(iv) Il Consiglio utilizza il termine *deduce* rischiando di far riferimento così ai soli sistemi che si avvalgono di un ragionamento *deduttivo* lasciando da parte i sistemi che seguono un processo di azione *induttivo*<sup>99</sup>.

(v) Il testo emendato fa riferimento alla deduzione che consentirebbe di raggiungere una determinata *serie* di obiettivi. Ciò rischierebbe di non includere nell'ambito di applicazione quei sistemi progettati e

---

95 Anche uno spazzolino da denti elettrico teoricamente sarebbe autonomo perché può operare senza un intervento umano, rischiando di includere quindi tecnologie che hanno poco a che fare con i sistemi IA. L'indipendenza dal controllo umano e l'interazione non sono sufficienti per parlare di autonomia. In questo senso, P. HACKER, *op. cit.*, p. 7. Secondo l'A. sarebbe necessario aggiungere il prerequisito dell'abilità della macchina di imparare e/o adattarsi autonomamente ad un nuovo ambiente. Invece, una nozione di *autonomia*, legata proprio ai sistemi IA, viene fornita dall'ISO negli Standard internazionali ISO/IEC 22989 del 2022 cit., la quale viene rappresentata come una caratteristica di un sistema che è in grado di modificare l'ambito di utilizzo o l'obiettivo previsto senza alcun intervento, controllo o supervisione esterna.

96 Si pensi ad esempio al grado di autonomia raggiunto negli scenari di guerra in cui vengono utilizzati droni autonomi come veri e propri robot-killer. Gli STM Kargu-2 sono dei droni di ultima generazione completamente autonomi che – secondo il rapporto dell'ONU del 8 marzo 2021 (S2021/229) – sono stati utilizzati per la prima volta dall'esercito turco in Libia nel marzo 2020. Nel rapporto si legge che «*The lethal autonomous weapons systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true "fire, forget and find" capability. The unmanned combat aerial vehicles and the small drone intelligence, surveillance and reconnaissance capability of HAF were neutralized by electronic jamming from the Koral electronic warfare system*». Il documento è consultabile al sito <https://digitallibrary.un.org/record/3905159?ln=en>, visitato l'ultima volta il 2 ottobre 2023, p. 17.

97 L'art. 14, par. 1, AIA, così come proposto dalla Commissione europea, prevede che «i sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso».

98 C. GRÖGER, *op. cit.*, pp. 98-108.

99 Sul ragionamento deduttivo e induttivo, oltre a quanto già esposto, si veda G. D'ACQUISTO, *Intelligenza artificiale*, Torino, 2021, pp.12 e ss.

sviluppati per il raggiungimento di un solo obiettivo.

(vi) Limita - eliminando il riferimento all'Allegato I - il riferimento ai soli sistemi che si avvalgono dell'apprendimento automatico e quelli basati sulla logica e sulla conoscenza rischiando perciò di non includere altri sistemi che, pur avvalendosi di altre tecniche, rientrerebbero nella scienza della IA.

(vii) La restante parte del testo emendato riproduce sostanzialmente quanto già proposto dalla Commissione, al di là della specificazione del fatto che con *contenuti* debba intendersi i sistemi di IA generativa.

Infine, con l'introduzione della definizione di Sistema IA per finalità generali si è introdotto un elemento aggiuntivo volto a fornire una disciplina ad essi pertinente e specificatamente applicabile. Tuttavia, non viene fornita una argomentazione esaustiva sulla ragione di questa nuova previsione, né si può dedurre il motivo di una nozione limitata a quei sistemi destinati a svolgere funzioni di applicazione generale di riconoscimento di immagini o vocale, creazione di audio o video, rilevazione di modelli, risposta a domande, traduzione o altro.

In conclusione, la proposta di testo avanzata dal Consiglio non risolve le criticità definitorie rilevate.

#### **10. (Segue) La proposta del Parlamento europeo e la "novità" riguardante i modelli di base.**

Il Parlamento europeo con il testo di Regolamento emendato e pubblicato il 14 giugno 2023 propone la seguente definizione di Sistema di IA all'art. 3 dell'AIA: «un sistema automatizzato progettato per operare con livelli di autonomia variabili e che, per obiettivi espliciti o impliciti, può generare output quali previsioni, raccomandazioni o decisioni che influenzano gli ambienti fisici o virtuali».

La proposta prevede una differente definizione anche di sistema IA per finalità generali: «un sistema di IA che può essere utilizzato e adattato a un'ampia gamma di applicazioni per le quali non è stato intenzionalmente e specificamente progettato».

Il Parlamento europeo inserisce anche una definizione di "modello di base" (*Foundation Model*): «un modello di sistema di IA addestrato su un'ampia scala di dati, progettato per la generalità dell'output e che può essere adattato a un'ampia gamma di compiti distinti».

Il testo proposto dal Parlamento europeo relativo alla nozione di sistema IA tenta di semplificare la struttura e, in parte, riesce a farlo.

Gli elementi di novità e modifica che possono essere sintetizzati afferiscono:

- (i) Al riferimento ad un sistema *automatizzato* abbandonando anche in questo caso, quindi, il riferimento al *software*.
- (ii) All'introduzione, anche in questo caso, dell'autonomia, ma facendo riferimento a *livelli variabili*.
- (iii) Agli obiettivi, che possono essere non solo espliciti, ma anche impliciti, senza specificare (non se ne vedrebbe la ragione) se debbano provenire dalla macchina o dall'uomo.
- (iv) All'eliminazione dei *contenuti* tra gli *output* generabili, probabilmente per l'introduzione della definizione dei "modelli di base" che attengono proprio alla IA generativa a cui si voleva alludere con il riferimento ai *contenuti*.
- (v) All'introduzione della specificazione che l'influenza degli ambienti può riguardare quelli fisici o virtuali. Questa specifica rafforzerebbe una interpretazione tesa a ritenere che l'influenza dell'ambiente con cui interagisce il sistema non debba arrivare al punto di modificare o influenzare il comportamento dell'utente.

Il Parlamento semplifica la definizione di sistemi IA per finalità generali prevedendo che si tratta di un sistema che si può adattare a una varietà generale di applicazioni per le quali non era stato in origine progettato e introduce un'altra tecnica riguardante i modelli di base (la IA generativa), soprattutto a seguito della diffusione (in particolar modo mediatica), di alcune applicazioni come Chat GPT e *Midjourney*<sup>100</sup>.

Anche i modelli di base meriterebbero una trattazione a sé; il termine è stato coniato dalla *Stanford Institute for Human-Centered Artificial Intelligence*<sup>101</sup> e sono Sistemi addestrati su una larga scala di dati come i programmi di elaborazione e comprensione del linguaggio naturale. Quindi, si va dagli assistenti digitali ai programmi *speech-to-text*. Sono sistemi che hanno consentito di costruire modelli generativi in grado di creare "nuove opere". Da qui derivano quindi i modelli di linguaggio naturale (NLP - *Natural Language Processing*) che possono essere sostanzialmente di due tipi: supervisionati o auto-supervi-

<sup>100</sup> L'emendamento riguardante questi modelli è stato presentato come una modifica necessaria per la nascita di una nuova tecnologia. In realtà, la tecnologia era già esistente, ma non era ancora così diffusa mediaticamente.

<sup>101</sup> *Stanford Institute for Human-Centered Artificial Intelligence - Center for Research on Foundation Models (CRFM), On the Opportunities and Risk of Foundation Models*, <https://crfm.stanford.edu>

sionati. Nella prima categoria rientrano quei modelli per i quali è necessario dotarli della risposta corretta per ogni *input*. La IA riceve, quindi, coppie di dati etichettati, l'*Input* e l'*Output* corretto; cosicché il sistema impara a produrre l'*output* che corrisponde a quell'*input* fornito.

Una versione più complessa è quella che passa dal riconoscimento alla comprensione. Per questo le parole devono essere "istanziate" come azioni (es. "Alexa metti su Bach" – Alexa deve capire che deve far iniziare un brano musicale di Bach). Per sistemi di questo tipo occorre molto tempo e risorse vista la miriade di modalità con cui l'uomo potrebbe esprimere una volontà o una proposta. Ogni possibile variazione nel chiarimento o nell'indicazione del dialogo deve essere presente nei dati di addestramento della Nlp. Non solo presente nei dati ma anche "etichettata" da un umano che fornisca sufficienti indizi per l'addestramento<sup>102</sup>.

La Nlp generale auto-supervisionata, invece, supervisiona sé stessa senza che sia necessaria alcuna *etichettatura* umana. È un approccio denominato "trasduzione di sequenza". In questi casi l'*input* sarebbe costituito dalla sequenza di tutte le parole fino a un certo punto, e l'*output* sarebbe semplicemente la sequenza di parole dopo quel determinato punto<sup>103</sup>.

Con dati sufficienti sarebbe un sistema c.d. *deep learning* in grado apprendere un linguaggio senza avvalersi di costrutti umani come la coniugazione e la grammatica, ma affidandosi ad astrazioni e costrutti che genera da sé, attingendo dai dati e incorporandoli in gigantesche reti neurali, senza alcuna *etichettatura*<sup>104</sup>.

In riferimento ai modelli di base, al di là della loro definizione legislativa, la novità di maggior rilevanza introdotta nella proposta del Parlamento europeo può essere rintracciata nell'art. 28-ter AIA dedicato

102 KAI-FU LEE, CHEN QIUFAN, *AI 2041*, Luiss University Press, 2023, p. 125-126.

103 *Ivi*, p. 126.

104 *Ivi*, p. 127. Gli A. aggiungono che Chat GPT-3 è stato addestrato con oltre 45 *tetrabyte* di dati di testo che richiederebbero circa 500mila vite per essere letti da una persona. Chat GPT ha quindi prodotto, dopo un lungo processo di addestramento, un gigantesco modello da 175 miliardi di parametri. Se si mostra una qualunque sequenza di parole a chat GPT, esso produrrà ciò che pensa possa seguire a queste parole. Esso, a differenza dell'uomo, non ha però la capacità di comprendere ciò che sa e ciò che non sa. È altresì debole nel ragionamento causale, nel pensiero astratto, nelle dichiarazioni esplicative, nel buon senso e nella creatività (intenzionale).

proprio agli obblighi del fornitore di un modello di base<sup>105</sup>.

### 11. I sistemi ad alto rischio. L'impianto proposto dalla Commissione europea.

Il fulcro della disciplina dell'AIA è rappresentato dai sistemi IA ad alto rischio individuati nell'art. 6 e nell'allegato III. La disciplina regolatoria individua una serie di requisiti essenziali in virtù dei quali deve accertarsi la conformità del dispositivo prima dell'immissione nel mercato e della messa in servizio. Il giudizio di conformità è rimesso agli attori coinvolti anziché a soggetti terzi come avviene in ambito farmaceutico dove è l'autorità amministrativa ad effettuare i test di sicurezza e a rilasciare l'autorizzazione preventiva<sup>106</sup>.

Dunque, una prima categoria è composta da quei sistemi IA che sono destinati ad essere utilizzati come componenti di sicurezza di un prodotto, o come prodotto, ai sensi di quelle normative che sono elencate nell'Allegato II della proposta di Regolamento e che siano soggetti ad una valutazione di conformità *ex ante* da parte di un soggetto terzo rispetto ai requisiti normativi in materia di sicurezza di prodotti<sup>107</sup>.

L'altra categoria di sistemi ad alto rischio è quella di cui al par. 2, il quale prevede che sono considerati

---

<sup>105</sup> La norma stabilisce che un fornitore di un modello di base è tenuto a garantire la conformità del sistema a determinati requisiti previsti, a prescindere dal fatto che sia fornito come modello autonomo o integrato in un sistema di IA o in un prodotto, o fornito su licenza gratuita e open source, come servizio, nonché altri canali di distribuzione. Vengono elencati quindi, al par. 2, sette requisiti piuttosto stringenti a cui il fornitore deve conformarsi. I successivi paragrafi, peraltro, prevedono ulteriori obblighi.

<sup>106</sup> G. RESTA, *Cosa c'è di 'europeo' nella proposta di regolamento UE sull'intelligenza artificiale?*, in *dir. inf. e inform.*, n. 2/2022, pp. 341-342. L'A. rileva come il sistema deve essere conforme a parametri di *data quality* stabiliti all'art. 10 AIA e che la conformità di un dispositivo è valutata alla stregua di tali parametri (art. 8). Il vero «ruolo nomotetico finirà per essere assunto dalle standard-setting organizations europee (...). Pur rimanendo in linea di principio possibile per i produttori o i fornitori di sistemi di IA prescindere dalle norme tecniche armonizzate, dando autonomo contenuto alla previsione legislativa, di fatto è soltanto tramite l'adeguamento ad esse che potrà ritenersi sussistente una presunzione di conformità alla stregua dell'art. 40 della proposta». Quindi, viene sottolineato come i veri 'legislatori' del settore diverranno *le standard setting organizations*.

<sup>107</sup> L'art. 6 della proposta di Regolamento della Commissione europea prevede che un sistema di IA è considerato ad alto rischio se sono soddisfatte due condizioni: «a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II; b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II». Per una sintesi riguardante la disciplina applicabile a questi sistemi si veda anche N. ABRIANI e G. SCHNEIDER, *op. cit.*, p. 109-111; sia consentito un rinvio anche a G. PROIETTI, *Una normativa per l'intelligenza artificiale. La proposta di regolamento europeo*, in *Riv. Tri. Resp. d'impresa e antiriciclaggio*, n. 2/2021, pp. 198 e ss.



ad alto rischio anche i sistemi IA inclusi nell'allegato III. In quest'ultimo allegato i sistemi ad alto rischio sono individuati in base ad un elenco di otto settori e di casi d'uso in cui sono destinati ad operare. In particolare:

1. Identificazione e categorizzazione biometrica delle persone fisiche:

a) i sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota "in tempo reale" e "a posteriori" delle persone fisiche.

2. Gestione e funzionamento delle infrastrutture critiche:

a) i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione del traffico stradale e nella fornitura di acqua, gas, riscaldamento ed elettricità.

3. Istruzione e formazione professionale:

a) i sistemi di IA destinati a essere utilizzati al fine di determinare l'accesso o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale;

b) i sistemi di IA destinati a essere utilizzati per valutare gli studenti negli istituti di istruzione e formazione professionale e per valutare i partecipanti alle prove solitamente richieste per l'ammissione agli istituti di istruzione.

4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicizzare i posti vacanti, vagliare o filtrare le candidature, valutare i candidati nel corso di colloqui o prove;

b) l'IA destinata a essere utilizzata per adottare decisioni in materia di promozione e cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti e per il monitoraggio e la valutazione delle prestazioni e del comportamento delle persone nell'ambito di tali rapporti di lavoro.

5. Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi:

a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica, non-

ché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi;

b) i sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA messi in servizio per uso proprio da fornitori di piccole dimensioni;

c) i sistemi di IA destinati a essere utilizzati per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi vigili del fuoco e assistenza medica.

6. Attività di contrasto:

a) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per effettuare valutazioni individuali dei rischi delle persone fisiche al fine di determinare il rischio di reato o recidiva in relazione a una persona fisica o il rischio per vittime potenziali di reati;

b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica;

c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per individuare i "deep fake" di cui all'articolo 52, paragrafo 3;

d) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per la valutazione dell'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati;

e) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi;

f) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati;

g) i sistemi di IA destinati a essere utilizzati per l'analisi criminale riguardo alle persone fisiche, che consentono alle autorità di contrasto di eseguire ricerche in set di dati complessi, correlati e non correlati, resi disponibili da fonti di dati diverse o in formati diversi, al fine di individuare modelli sconosciuti o

scoprire relazioni nascoste nei dati.

7. Gestione della migrazione, dell'asilo e del controllo delle frontiere:

a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica;

b) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti per valutare un rischio (compresi un rischio per la sicurezza, un rischio di immigrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro;

c) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti per verificare l'autenticità dei documenti di viaggio e dei documenti giustificativi delle persone fisiche e per individuare i documenti non autentici mediante il controllo delle caratteristiche di sicurezza;

d) i sistemi di IA destinati ad assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status.

8. Amministrazione della giustizia e processi democratici:

a) i sistemi di IA destinati ad assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti.

Al di là della scelta di includere l'uno o l'altro settore nell'ambito dell'Allegato III, ciascuno di essi meriterebbe una analisi a sé, in questa sede inopportuna.

Il Consiglio d'Europa ha apportato modifiche anche in riferimento all'art. 6 e all'allegato III.

## **12. (Segue) I sistemi ad alto rischio secondo il Consiglio d'Europa e il Parlamento europeo.**

La modifica apportata dal Consiglio con l'introduzione del par. 3 dell'art. 6 AIA contiene nuove disposizioni in forza delle quali, nella classificazione dei sistemi, bisogna prendere in considerazione anche la rilevanza dei risultati del sistema rispetto all'azione pertinente o alla decisione da adottare. Questa rilevanza deve essere valutata a seconda che essa sia o meno accessoria rispetto all'azione o alla decisione da adottare. Spetterebbe alla Commissione specificare le circostanze in cui gli *output* dei sistemi di IA di cui all'allegato III sarebbero puramente accessori rispetto alla pertinente azione o decisione

da adottare attraverso atti di esecuzione<sup>108</sup>. Il par. 3 dell'art. 6 AIA prevede, quindi, un ulteriore livello orizzontale volto a garantire che non vengano inclusi quei sistemi IA che non presentano il rischio di causare gravi violazioni dei diritti fondamentali o altri rischi significativi.

Nella relazione di accompagnamento della proposta del Consiglio si legge che tre dei casi d'uso di IA ad alto rischio presenti nell'allegato III sono stati soppressi, ossia l'individuazione dei "deep fake" da parte delle autorità di contrasto, l'analisi criminale, la verifica dell'autenticità dei documenti di viaggio; due settori/casi d'uso sono stati aggiunti, ossia le infrastrutture digitali critiche e l'assicurazione sulla vita e sanitaria. Altri, invece, sono stati "perfezionati".

Il Parlamento europeo dal canto suo ha apportato ulteriori e rilevanti modifiche.

È stata parzialmente modificata la condizione di cui alla lett. b) del par. 2 dell'art. 6 AIA introducendo il riferimento ai rischi per "la salute e la sicurezza". In altri termini, quando il prodotto è soggetto alla valutazione della conformità da parte di terzi, tale valutazione deve riguardare i rischi per la salute e la sicurezza. Quindi, rispetto alle altre due proposte, il perimetro di applicazione è più ristretto.

Il par. 2, così come modificato, prevede che sono considerati ad alto rischio quei sistemi di IA che rientrano in uno o più settori critici e casi d'uso di cui all'allegato III se sussiste un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche<sup>109</sup>. Qualora un sistema di IA rientri nell'allegato III, punto 2 (gestione e funzionamento delle infrastrutture critiche) è considerato ad alto rischio solo se presenta un rischio significativo di danno per l'ambiente. Il comma 2 prevede inoltre che, sei mesi prima dell'entrata in vigore del Regolamento, la Commissione, previa consultazione dell'ufficio per l'IA e dei pertinenti portatori di interessi, è tenuta a fornire orientamenti volti a specificare chiaramente le circostanze in cui l'*output* dei sistemi di IA inclusi nell'allegato III pro-

---

<sup>108</sup> Il par. 3 prevede testualmente che «i sistemi di IA di cui all'allegato III sono considerati ad alto rischio a meno che l'output del sistema non sia puramente accessorio in relazione alla pertinente azione o decisione da adottare e non sia pertanto suscettibile di comportare un rischio significativo per la salute, la sicurezza o i diritti fondamentali». Il comma 2 prevede che per «garantire condizioni uniformi di esecuzione del presente regolamento, la Commissione adotta, entro un anno dall'entrata in vigore del presente regolamento, atti di esecuzione per specificare le circostanze in cui gli output dei sistemi di IA di cui all'allegato III sarebbero puramente accessori rispetto alla pertinente azione o decisione da adottare. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2».

<sup>109</sup> L'introduzione del rischio "significativo" ha dato vita a differenti opinioni tra associazioni e dottrina. Alcuni apprezzano la novità poiché considererebbe di differenziare i sistemi a seconda dei casi d'uso concreti in termini di rischio alla persona; in questo senso, P. HACKER, *op. cit.*, p. 7.

durrebbero il suddetto rischio significativo.

Il Parlamento europeo ha peraltro aggiunto il par. 2 *bis* secondo il quale «se i fornitori che rientrano in uno o più dei settori critici e dei casi d'uso di cui all'allegato III ritengono che il loro sistema di IA non presenti un rischio significativo come descritto al precedente paragrafo, possono presentare all'autorità nazionale di vigilanza una notifica motivata attestante che non sono soggetti ai requisiti di cui al titolo III, capo 2, del regolamento».

In caso di errore nella classificazione di un sistema IA da parte dei fornitori – ossia come non soggetto ai requisiti di cui al titolo III, capo 2, del Regolamento – sarebbero soggetti a sanzioni pecuniarie a norma dell'articolo 71 (par. 2 *ter*).

L'allegato III – così come modificato dal Parlamento europeo – propone sempre otto settori e casi d'uso apportando qualche modifica e novità.

Alcune modifiche apportate dal Consiglio e dal Parlamento sono state recentemente oggetto di dura critica in una lettera aperta da parte di 118 associazioni che hanno rilevato come gli emendamenti darebbero vita ad una *scappatoia* per gli operatori di sistemi IA ad alto rischio<sup>110</sup>. In particolare, viene rappresentato che l'articolo 6 così come emendato consentirebbe agli sviluppatori di IA di decidere di esentarsi da tutte le norme sostanziali per i sistemi ad alto rischio creando un'elevata incertezza giuridica su quali sistemi siano considerati "ad alto rischio"; ci sarebbe una frammentazione del mercato unico dell'UE, con interpretazioni diverse su ciò che si intende per "rischio elevato" tra gli Stati membri; verrebbe consentito a quegli sviluppatori più spregiudicati di evitare i requisiti di base della legge volti a rendere i loro sistemi più sicuri e affidabili ponendo in una posizione di svantaggio quelli più responsabili<sup>111</sup>.

Da una lettura complessiva della proposta regolatoria emerge che alcuni settori e casi d'uso sono stati omessi ed altri sono stati parzialmente inseriti, ossia tramite il rinvio all'allegato II, quindi ai sensi del

<sup>110</sup> EU legislators must close dangerous loophole in AI Act, consultabile al sito [beuc.eu](http://beuc.eu)

Nella lettera aperta si legge testualmente che «In the original draft from the European Commission, an AI system was considered 'high risk' if it was to be used for one of the high-risk purposes listed in Annex III. However, the Council and the European Parliament have introduced a loophole that would allow developers of these systems decide themselves if they believe the system is 'high-risk'. The same company that would be subject to the law is given the power to unilaterally decide whether or not it should apply to them».

<sup>111</sup> *Ibidem*.

primo paragrafo dell'art. 6 AIA.

Tra quegli ambiti che risultano non rientrare nel perimetro dell'alto rischio balza all'occhio il settore farmaceutico, in cui gli sviluppi e l'uso dell'intelligenza artificiale sono già esistenti e ambiziosi; l'ambito finanziario, come ad esempio i cc.dd. algoritmi ad alta frequenza<sup>112</sup>; l'ambito e l'uso delle piattaforme on-line come i *social network*, i motori di ricerca e l'ambito dell'*e-commerce*, la cui ragione può essere rintracciata nella loro sottoposizione al già vigente *Digital Services Act*<sup>113</sup>; l'ambito medico-sanitario e quello agricolo, invece, sembrerebbero rientrare in parte nella categoria ad alto rischio. Il primo, attraverso il richiamo (nell'allegato II) del Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro, mentre il secondo attraverso il richiamo del Regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio, del 5 febbraio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli agricoli e forestali (GU L 60 del 2.3.2013, pag. 1).

Per quanto riguarda l'ambito medico-sanitario, la diagnostica in vitro costituisce una parte essenziale dell'assistenza sanitaria, ma il perimetro entro cui poter considerare un sistema ad alto rischio rispetto alla diffusione nel settore dei sistemi IA risulta ben più esteso. Il settore sanitario rientra anche attraverso il n. 5 dell'Allegato III che, soprattutto nella versione modificata dal Parlamento europeo, include la sanità ma solo per quanto riguarda i sistemi IA destinati al loro utilizzo da parte delle autorità per valutare l'accesso anche ai servizi sanitari.

Un altro settore che viene fatto rientrare solo parzialmente nel perimetro dei sistemi ad alto rischio, con un margine quindi limitato, riguarda quello dell'*automotive* e dei droni che vengono delineati tramite il richiamo – all'allegato II – di normative settoriali come il Regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi e del Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea. Da questa "esclusione" se ne può ricavare una discrasia rispetto all'ultima e più recente raccomandazione adottata dalla Commissione europea sui settori

<sup>112</sup> Su questo tema in particolare si veda P. LUCANTONI, *L'high frequency trading nel prisma della vigilanza algoritmica del mercato*, in *Analisi giuridica dell'economia*, n. 1/2019, p. 297.

<sup>113</sup> Su questa normativa si veda L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), *Digital Services Act e Digital Markets Act*, Milano, 2023; sia consentito il rinvio anche a G. PROIETTI, *Il Digital Services Act: la normativa sui servizi digitali*, in *dirittobancario.it*, 12 giugno 2023.

tecnologici critici per la sicurezza economica dell'UE che include anche i droni e veicoli<sup>114</sup>. Infine, alcuni hanno indicato, come caso d'uso mancante e ritenuto meritevole di inclusione, anche quello riguardante la sicurezza nazionale e le agenzie di intelligence<sup>115</sup>.

Va da sé che la scelta di includere l'uno o l'altro settore, per quanto possa essere discutibile e criticabile, rimane ascritta ad una decisione politica del legislatore. Ciò che può essere criticato sotto un profilo squisitamente giuridico attiene ad una coerenza di principio che nelle politiche del diritto occorre pur sempre seguire. In altri termini, il dichiarato perseguimento di una tutela dei diritti fondamentali per la creazione di un ecosistema di fiducia verso i sistemi IA dovrebbe coerentemente includere quegli ambiti in cui la ricerca in tema di IA è profusa e sono strettamente legati a tali diritti, quindi l'esclusione del settore farmaceutico e sanitario suscita ineluttabilmente qualche perplessità.

### **13. Lo strumento computazionale capace di conseguire uno o più risultati avvalendosi di tecniche simboliche o sub-simboliche.**

Come si è avuto modo di vedere, il tentativo di fornire una definizione di intelligenza artificiale è risalente. Negli anni recenti anche la giurisprudenza si è pronunciata operando una distinzione, più o meno condivisibile, tra algoritmo e intelligenza artificiale intendendo, con il primo, quei sistemi il cui funzionamento segue strategie algoritmiche, ossia istruzioni predeterminate per il raggiungimento di

---

114 Il riferimento è alla recente raccomandazione del 3 ottobre 2023 *On critical technology areas for the EU's economic security for further risk assessment with Member States*, con la quale la Commissione ha presentato un elenco di dieci settori tecnologici critici (tra cui, oltre all'Intelligenza artificiale, vengono inclusi i droni e i veicoli autonomi); di questi dieci settori vengono a loro volta selezionati quattro settori tecnologici (semiconduttori avanzati - intelligenza artificiale - tecnologie quantistiche - biotecnologie) e viene raccomandato che gli Stati membri, congiuntamente alla Commissione, effettuino entro la fine dell'anno corrente le valutazioni dei rischi collettivi per i settori stessi.

115 N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI, K. YEUNG, *How the EU can achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, in *Leads Lab @University of Birmingham*, 2021, p. 55.

un dato obiettivo; con IA, invece, ci si rifà ai sistemi di apprendimento automatico<sup>116</sup>.

Tra i vari tentativi, la definizione che trova maggior consenso è probabilmente quella elaborata dall'OCSE da cui hanno tratto ispirazione molte altre istituzioni, tra le quali anche l'ISO<sup>117</sup>.

Un sistema IA, secondo la definizione dell'OCSE, resa con raccomandazione del 22 maggio 2019, è «un sistema basato su una macchina che, per un determinato insieme di obiettivi definiti dall'uomo, può fare previsioni, raccomandazioni o decisioni che influenzano ambienti reali o virtuali. I sistemi di IA sono progettati per operare con vari livelli di autonomia»<sup>118</sup>.

Le proposte legislative europee per alcuni aspetti si ispirano alla definizione OCSE, come ad esempio le tipologie di risultati che i sistemi possono realizzare (raccomandazioni, previsioni ecc.) così come per l'influenza degli ambienti reali o virtuali e l'autonomia. Uno degli intenti del legislatore che lo hanno indotto all'iniziativa normativa è quello di farsi promotore di un modello regolatorio che possa fungere da paradigma per altre realtà globali, tentando quindi di tutelare i diritti a fronte dei rischi derivanti dallo sviluppo e dalla diffusione di certi sistemi IA, senza pregiudicare le istanze dell'innovazione.

Tra i vari rischi, uno dei principali potrebbe essere rintracciato in un "effetto calcolatrice", consistente nella persistente delega di funzioni a sistemi tecnologici tale da produrre un significativo "indebolimen-

---

116 Il riferimento è alla Sentenza del Consiglio di Stato, 25/11/2021, n. 7891, quot. giurid. 2021, con la quale è stato affermato che con "algoritmo" si intende semplicemente «una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato (come risolvere un problema oppure eseguire un calcolo e, nel caso di specie, trattare un'aritmia)»; con intelligenza artificiale, invece, secondo il Consiglio di Stato, ci si riferisce «allo studio di "agenti intelligenti", vale a dire allo studio di sistemi che percepiscono ciò che li circonda e intraprendono azioni che massimizzano la probabilità di ottenere con successo gli obiettivi prefissati (...) sono tali, ad esempio, quelli che interagiscono con l'ambiente circostante o con le persone, che apprendono dall'esperienza (*machine learning*), che elaborano il linguaggio naturale oppure che riconoscono volti e movimenti».

117 Quest'ultima, nel ISO/IEC 22989 cit., riporta la seguente definizione di sistema IA: «*engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives*». Nella nota a tale definizione viene aggiunto che «*The engineered system can use various techniques and approaches related to artificial intelligence to develop a model to represent data, knowledge, processes, etc. which can be used to conduct tasks*».

118 Raccomandazione del Consiglio dell'Organizzazione per la cooperazione e lo sviluppo economici (OCSE), del 22 maggio 2019, sull'intelligenza artificiale.



to" cognitivo dell'utilizzatore umano<sup>119</sup>.

Tra le scelte politiche rientra quella di voler fornire una definizione di sistema di IA che, tuttavia, appare complessa nei suoi elementi e suscettibile di generare difficoltà ermeneutiche; di essere eccessivamente inclusiva o poco precisa. Si è visto come a volte si è fatto riferimento al sistema IA come un *software* oppure semplicemente come un "sistema" o ancora un "sistema automatizzato", quando sembrerebbe pacifico che si possa parlare di uno strumento computazionale, senza che ciò trascuri qualche elemento tecnico imprescindibile.

Il riferimento a quali risultati il sistema debba produrre, finendo per tipizzarli, non sembra possa portare importanti vantaggi e utilità, essendo quindi sufficiente parlare di *risultati*; così come non sembra necessario, ai fini legali, il riferimento ad obiettivi che vengano stabiliti dall'uomo o dalla macchina. Sembrerebbe piuttosto opportuno, per soddisfare il requisito della precisione e il principio della certezza del diritto, inquadrare in modo semplice – senza pregiudicare l'elemento della flessibilità – le tecniche e gli approcci in presenza delle quali si può parlare di IA. Definendo, perciò, in modo obiettivo e concreto il perimetro dell'ambito di applicazione. La Commissione europea, come è stato criticato da molti, operava questo inquadramento in modo piuttosto discutibile, mentre potrebbe essere utile limitare il riferimento – anche se verrebbe inevitabilmente ridotto il perimetro della comprensibilità – alle due classi entro le quali un sistema può essere considerato una IA, ossia le tecniche simboliche e sub-simboliche. Dunque, un sistema di IA potrebbe essere considerato come lo strumento computazionale capace di conseguire uno o più risultati avvalendosi di tecniche simboliche o sub-simboliche.

---

<sup>119</sup> Il riferimento alla calcolatrice non vuole essere casuale. Nel 1966 molti insegnanti di matematica protestarono nelle strade statunitensi contro l'utilizzo nelle scuole della calcolatrice come mezzo per la soluzione di operazioni di calcolo matematici rilevando come ciò potesse provocare un detrimento delle capacità degli studenti.